MANNING

Windows PowerShell 实战指南

（第2版）

Learn WINDOWS POWERSHELL IN A MONTH OF LUNCHES Second Edition

〔美〕 Don Jones　Jeffery Hicks　著

宋沄剑 何文通 黄钊吉 陈畅亮　译



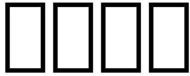
中国工信出版集团



人民邮电出版社

POSTS & TELECOM PRESS





Windows PowerShell 2

ISBN 978-7-115-40967-6

[ ] Don Jones Jeffery Hicks

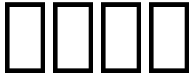
11

100164 315@ptpress.com.cn

http://www.ptpress.com.cn

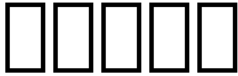
(010)81055410

(010)81055315



[illegible]

PowerShell[illegible]Shell[illegible]PowerShell[illegible]Windows[illegible]1[illegible]1[illegible]1[illegible]PowerShell[illegible]PowerShell[illegible]Don Jones[illegible]Jeffery Hicks[illegible]PowerShell MVP[illegible]



[illegible] PowerShell[illegible]

——Chuck Durfee

Graebel[illegible]

[illegible] Don Jones [illegible] PowerShell [illegible]

——David Moravec

[illegible] PowerShell.cz [illegible] SCCM [illegible]

[illegible] PowerShell [illegible]

——Ray Booysen

[illegible] BNP Paribas [illegible]

[illegible] PowerShell [illegible]

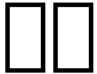
——Richard Siddaway

[illegible] PowerShell MVP [illegible] IT [illegible]

[illegible] PowerShell [illegible] PowerShell [illegible]

——Nikander Bruggeman [illegible] Margriet Bruggeman

Lois & Clark IT [illegible] .NET [illegible]



[illegible]PowerShell[illegible]Don[illegible]PowerShell[illegible]——[illegible]——[illegible]Shell[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]

[illegible]Don[illegible]WindowsITPro.com[illegible]——[illegible]PowerShell v3[illegible]Don[illegible]Jeffery Hicks[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]Exchange Server[illegible]SQL Server[illegible]System Center[illegible]Shell[illegible]PowerShell[illegible]PowerShell[illegible]“cookbook”[illegible]

[illegible]PowerShell[illegible]MoreLunches.com[illegible]PowerShell[illegible]Learn PowerShell Toolmaking in a Month of Lunches[illegible]PowerShell[illegible]

[illegible][www.PowerShell.org][illegible]www.PowerShell.org[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]

[illegible]——[illegible]Shell[illegible]

[illegible]

[illegible]1[illegible]

[illegible]Windows 8[illegible]Windows Server 2012[illegible]1[illegible]Windows 7 [illegible] Windows 8.1[illegible]Windows Server 2012 R2[illegible]Windows PowerShell[illegible]

[illegible] [illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]http://Morelunches.com[illegible]“[illegible]”[illegible] www.manning.com/LearnWindowsPowerShellinaMonthofLunchesSecondEdition[illegible]

[illegible]

```
Get-WmiObject –class Win32_OperatingSystem
➥ –computerName SERVER-R2
```

[illegible]PowerShell[illegible]Win32_OperationSystem[illegible]——[illegible]PowerShell[illegible]

[illegible]Get-Command[illegible]Shell[illegible]

[illegible] `[illegible]

```
Invoke-Command –scriptblock { Dir } `
-computerName SERVER-R2,localhost
```

[illegible]——[illegible]Esc[illegible]~[illegible]——[illegible]——[illegible]Tab[illegible]Tab[illegible]

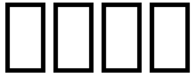
[illegible]Internet[illegible]URL[illegible]URL[illegible]Manning[illegible]http://mng.bz/S085[illegible]1[illegible]

[illegible]

[illegible]Learn Windows PowerShell in a Month of Lunches[illegible]Second Edition[illegible]Manning[illegible]www.manning.com/LearnWindowsPowerShellinaMonthofLunchesSecondEdition[illegible]www.manning.com/jones3[illegible]Author Online[illegible]

Manning[illegible]

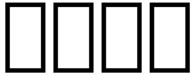
[illegible]



[illegible]PowerShell[illegible]Don Jones[illegible]Jeffery Hicks[illegible]
PowerShell MVP[illegible]Don[illegible]
PowerShell.org[illegible]Jeff[illegible]jdhitsolutions.com/blog[illegible]

[illegible]Don Jones[illegible]Windows PowerShell[illegible]MVP[illegible]TechNet[illegible]Windows PowerShell[illegible]PowerShell.org[illegible]“Decision Maker”[illegible]Redmond[illegible]Don[illegible]2001[illegible]12[illegible]Concentrated Technology (ConcentratedTech.com)[illegible]IT[illegible]Don[illegible]Windows[illegible]KiXtart[illegible]20[illegible]90[illegible]1995[illegible]VBScript[illegible]“Monad”[illegible]IT[illegible]——[illegible]Windows PowerShell[illegible]Don[illegible]IT[illegible]PowerShell[illegible]IT[illegible]

Jeffery Hicks[illegible]Windows PowerShell[illegible]20[illegible]IT[illegible]Jeffery[illegible]MPCMag.com[illegible]Prof.PowerShell[illegible]Petri IT[illegible]TrainSignal[illegible]Jeffery[illegible]http://jdhitsolutions.com/blog[illegible]



[illegible]SQL Server MVP[illegible]SQL Server 2012 UI[illegible]Professional Association for SQL Server(PASS)[illegible]TechED[illegible]50[illegible]/[illegible]

[illegible]MS SQL[illegible]MS SQL[illegible]

[illegible]8[illegible]SQL Server[illegible]SQL Server MVP[illegible]CSDN[illegible]SQL[illegible]CSDN[illegible]SQL Server[illegible]

[illegible]SQL Server MVP[illegible]2015[illegible]DTCC[illegible]SQL Server[illegible]SQL Server[illegible]MySQL[illegible]NoSQL[illegible]

□□

□□□□□□□□□□□□□□□□□□□□Don□□□□□□Manning□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Jeffery□□□□□Don□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□Don□Jeffery□□Manning□□□□□□□□□□“□□□□□□□”□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Bennett Scharf, Dave Pawson, David Moravec,Keith Hill, and Rajesh Attaluri□□□□□James Berkenbile □Trent Whiteley□□□□□□□□□□□□□□□

[illegible]1[illegible] [illegible]

[illegible]2006[illegible]Windows PowerShell[illegible]PowerShell[illegible]VBScript[illegible]VBScript[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]2009[illegible]VBScript[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

1.1 [illegible]PowerShell

[illegible]Batch[illegible]KiXtart[illegible]VBScript[illegible]Windows PowerShell[illegible]Windows[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell

Windows[illegible]GUI[illegible]Windows[illegible]——[illegible]“[illegible]”[illegible]GUI[illegible]GUI[illegible]GUI[illegible]5[illegible]

[illegible]100[illegible]500[illegible]——[illegible]

[illegible]VBScript[illegible]VBScript[illegible]CSV[illegible]VBScript[illegible]VBScript[illegible]VBScript[illegible]IP[illegible]VBScript[illegible] Jeffery Snover[illegible]Windows PowerShell[illegible]“[illegible]”[illegible]VBScript[illegible]“[illegible]”[illegible]

Windows PowerShell[illegible]“[illegible]”[illegible]

[illegible]PowerShell

[illegible]Windows PowerShell[illegible]Shell[illegible]Windows[illegible]GUI[illegible]PowerShell[illegible]Shell[illegible]Windows[illegible]GUI[illegible]Shell[illegible]

[illegible]Exchange Server 2007[illegible]2010[illegible]Sharepoint Server 2010[illegible]System Center[illegible]Windows[illegible]Windows[illegible]Shell[illegible]Windows Server 2012[illegible]PowerShell V3[illegible]PowerShell[illegible]PowerShell[illegible]GUI[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]IT[illegible]GUI[illegible]IT[illegible]AS/400[illegible]Unix[illegible]“[illegible]”[illegible]Windows[illegible]PowerShell[illegible]Don[illegible]2010TechEd[illegible]“[illegible]PowerShell”[illegible]“[illegible]”[illegible]

[illegible]PowerShell[illegible]

1.2 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible]Shell[illegible]Shell[illegible]Shell[illegible]

[illegible]PowerShell[illegible]Shell[illegible]

[illegible]PowerShell[illegible]WMI[illegible]Windows Management Instrumentation[illegible]PowerShell[illegible]PowerShell[illegible]

1.3 [illegible]

[illegible]40[illegible]20[illegible]

[illegible]

[illegible]2[illegible]25[illegible]24[illegible]

[illegible]

[illegible]

[illegible] MoreLunches.com [illegible]

[illegible]

MoreLunches.com [illegible] PowerShell [illegible]

[illegible]

[illegible]

[illegible]

[illegible] PowerShell [illegible] Shell [illegible] “[illegible]” [illegible]

1.4 [illegible]

[illegible] PowerShell [illegible]

[illegible] PowerShell [illegible] Windows [illegible] Windows Vista [illegible] Windows 7 [illegible] Windows Server 2008 [illegible]

Windows Server 2008 R2□Windows 8□□□Windows Server 2012□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□PowerShell□□□□□□□□□□□□□□□□□□PowerShell□Windows□□□□□□□□□□□□□Windows 8 □□Windows Server 2012□PowerShell□□□Windows 8□□Windows Server 2012□□□PowerShell□□□□□□□□□□

□□□□□□□□64□□X64□□□□□□□□□□□□□□□□□□□□Windows PowerShell□□□□□□□□□Windows PowerShell ISE□□□□□□Windows 8□□□“□□”□□□□□□□□64□□□□“Windows PowerShell”□“Windows PowerShell ISE”□32□□□□□□□□□□□“X86”□□□□X86□□PowerShell□□□□□□□□□X86□□□□□□□□□□□32□□□□□□□□32□□PowerShell□□□□□X86□□□

□□□□□□□64□□□□PowerShell□□□ISE□□□□□□□□□□64□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□32□□□□PowerShell□□□□□□□□□□□□□□Shell□□□□□□□□32□PowerShell□□□□□□□□32□□□X86□□Shell□□□□□□□□□□□□□□□□□□□□□□□64□□□□□□□64□□PowerShell□□□□□□□□□□□64□PowerShell□□□□□□□□□□32□□□□□□□□□□□□□□□□□□□□□□□□□□

> □□□ □□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CloudShare.com□□□CloudShare.com□□□□□□□□□□□

1.5 □□Windows PowerShell

□Windows Server 2008□Windows Server 2008 R2□Windows 7□□□□□□□□□□□□□□□□Windows PowerShell□Windows Vista□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□Windows PowerShell□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□

> □□□ □□□□□□□□□□□□PowerShell□□□□PowerShell□□□□□$PSVersionTable□□□□□□□□□□□□□□□□□□□□“PSVersion 3.0”□□□□□□□□□□□□

PowerShell□

□□□PowerShell□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□

□□□□□□□□□□□PowerShell□□□□□
http://download.microsoft.com□□□□□□□□□□□PowerShell 3□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□Windows Management Framework□□□□PowerShell□□X86□□32□□□□□□X64□□64□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□

> □□□ PowerShell□□□□.Net Framework V4,□□□□□□□□□□□□□□Framework□□□□□□□□□□□□□□□□□□.Net Framework 3.5 SP1□□.Net Framework 4.5□□□□□□□□□□PowerShell□□□□□□

□□PowerShell□□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□WinRM□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□Hotfix□□□PowerShell□□□□□□□□Windows □□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□Windows□□□□□□Windows□hotfix□□SP□□□□□□□

PowerShell□□□□□□□□□□□□□□□□□□□□□□□PowerShell.exe□□□□□□□□□□□□□□□□□□□□□ISE□PowerShell_ISE.exe□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ISE□□□□□□□□□

> □□□ PowerShell ISE□□□□□□□□□□Server□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□"□□□□□□□"□□□□□□□□□□ISE□□□□□□□□□□□□PowerShell□□□□□□□□□□Add-WindowsFeaturePowerShell -ise□□□□□□□□□□GUI□□□□□□□□□□□Server Core□□□□□□□□□□□□□□□□□□□□□□□□□ISE□□□□□□□

□□□□□□PowerShell□□□□□□□□□□□□□□□□Shell□□Lucida□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□1□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

[illegible]2[illegible]

> **[illegible]** [illegible]

[illegible]

1.6 [illegible]

[illegible]MoreLunches.com[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]Windows PowerShell[illegible]
- Don[illegible]Windows PowerShell FAQ[illegible]
- [illegible]

[illegible]PowerShell[illegible]MoreLunches.com[illegible]

[illegible]http://jdhitsolutions.com/blog[illegible]Twitter[illegible]@jeffhicks[illegible]Jeffery[illegible]

1.7 [illegible]PowerShell[illegible]

“[illegible]”[illegible]20[illegible]MoreLunches.com[illegible]

□2□ □□PowerShell

□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

2.1 □□□□“□□”

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□2.1□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□

> **□□□** □□□□□Windows□□□□□□□□Windows Server 2012□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□>□□□□>□Windows PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□“PowerShell.exe”□□□□□□□□□□ □□PowerShell□□□□□□□□□□Windows 8□Windows Server 2012□□□□Windows□□□□□□Ctrl□□Alt□□□□Windows□□□□R□□□□□□□□□□□□□Windows□□□□□□□□□□□PowerShell□□□□□□□PowerShell□□□

□32□□□□□□□□□□□□□□PowerShell□□□□64□□□□□□□□4□□□□□□□□

- Windows PowerShell——64□□□□□64□□□□□32□□□□□32□□□□□
- Windows PowerShell(x86)——64□□□□□32□□□□□
- Windows PowerShell ISE——64□□□□□64□□□□□□□□32□□□□□32□□□□□□□□
- Windows PowerShell(x86)——64□□□□□32□□□□□□□□



□2.1　□□□□□□□PowerShell□□□□□□□□□

□□□□□32□□□□□□□32□□PowerShell□□□□□□64□□□□□□□□32□□64□□□□□□PowerShell□□□□□□□32□□□□□□□□□□□□□“x86”□□□□□□□□□□□□□□□□□□□□□32□□□□□□□64□□□□□□□□□□□□□□□64□□□□□□32□□□□□□□□□

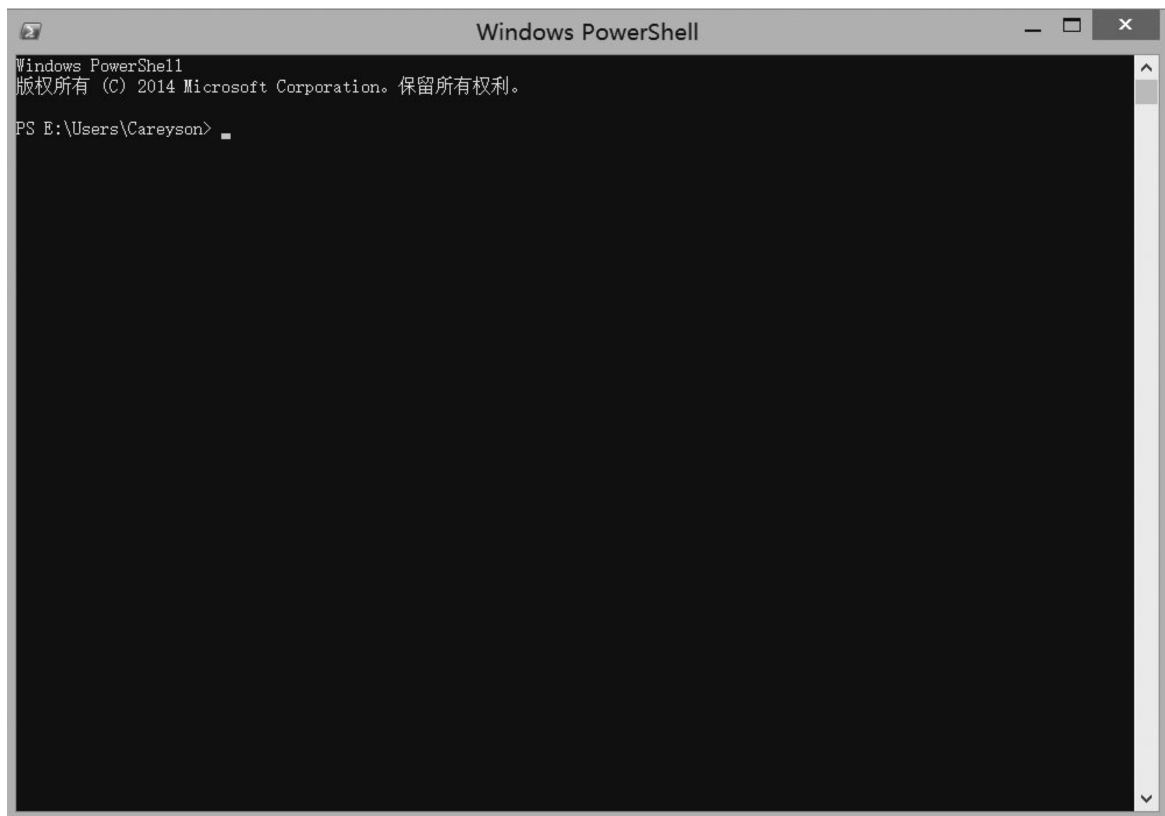
□□□　□64□□□□□□□□□□□□□□□□□32□□□□□□□□□□□□□□□□□□□□□□□□□“x86”□□□□□□□□32□□□□□□□64□□□□□□□□□□□32□□□□□□□□□□□□□□□□64□□□□□□□□□□□□□□□□□□□□□□□□□

2.1.1　□□□□□

□2.2□□□PowerShell□□□□□□□□□□□□□□□□□□□□PowerShell□□□

□□□□□□□□□PowerShell□□□□□□□□□□□□□□

- PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- PowerShell□□□□□□□□□□□□□□□□□□□ISE□□□□□□□□□□□□



□2.2　□□□PowerShell□□□□□□PowerShell.exe

□□□□□PowerShell□□□□□□□□□□□□□□□□GUI Shell□□□□□□□PowerShell□□□□□□□□□□“□□□□□□□”□□□□Windows Server□□□□GUI Shell□□□□□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□PowerShell□□□□□.NET Framework□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□20□□70□□□□□□□□□□□□□

□□2.3□□□

□□□□□□□□□□□□□□□□□“□□□□”□□□F7□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□12□□□□□□□□□□□□□□□□□1.5□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□’□□□□□□□□□□□`□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□



图2.3 [illegible]

[illegible]“[illegible]”[illegible]PowerShell[illegible]

[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]1985[illegible]

2.1.2 [illegible]ISE[illegible]

[illegible]2.4[illegible]PowerShell [illegible]ISE[illegible]

[illegible]

□□□□□□□□□□□□□□□□□□□□□□□□□□“ise”□□□□□□□□□□ISE□

□2.4　PowerShell ISE□PowerShell_ISE.exe□

□2.1　ISE□□□□

□□	□□
ISE□□□□□□□□□□□□□	ISE□□Windows Presentation Foundation □WPF□□□□□□□□□□□□GUI□□□□□□ISE
□□□□□□□□ISE□□□□□ PowerShell□□□□□□□□□□□□	□□□□□□□□□□□□□□□□□□□□□□□□□□
ISE□□□□□□□□□□□□	ISE□□□□□

□2.1□□□ISE□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□2.5□□□ISE□□□□□□□□□□□□□□□□□□□ISE□□□□□

□□2.5□□“X”□□

[illegible]

[illegible]ISE[illegible]——[illegible]

[illegible]2.5　ISE[illegible]

[illegible]ISE[illegible]ISE[illegible]

2.2　[illegible]

PowerShell[illegible]PowerShell[illegible]

[illegible]

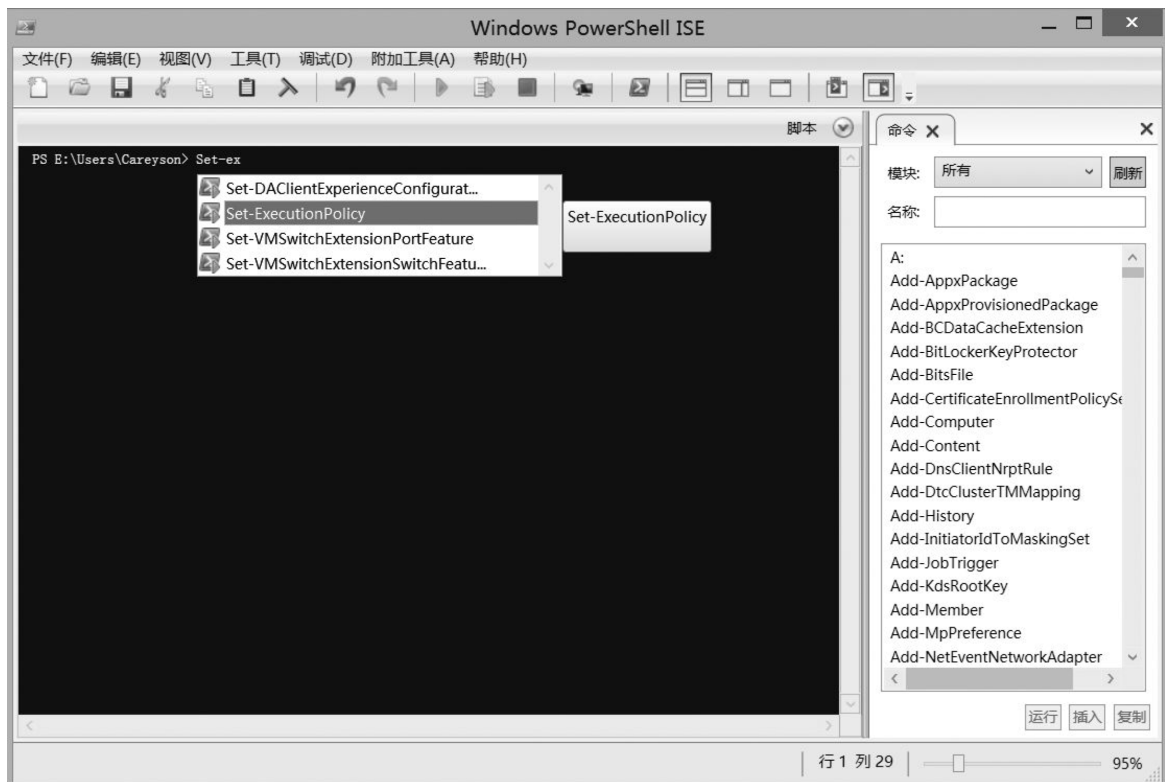
□□□□□□□□□□□“Tab□□□”□

- □□“Get-S”□□□□□□“Tab”□□□□Shift+Tab□□□□PowerShell□□□□□□ Get-S□□□□□□□□□□□□□□Shift+Tab□□□□□□□□□□□□□□□□□□□
- □□“Dir”□□□□□□□□□□□C:\□□□“Tab”□□PowerShell□□□□□□□□□□□□□□ □□□□□□□□□□□□□
- □□“Set-Execu”□□“Tab”□□□□□□□□□□□□□□□-□□□□□□“Tab”□□□□□□ PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□-E□□□ □“Tab”□□□□□□□□□□□□□□“Esc”□□□□□□□□□
- □□□□“Set-Execu”□□“Tab”□□□□□□□□□□□□-E□□□□“Tab”□□□□□□□□□ □□□□“Tab”□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□“Esc”□□□□□□□□□□□□

PowerShell ISE□□□□□□□□□□□□□□□“Tab□□”□□□□□□□——□□□□□□□□ □□□□□□□□□□□□□□□□2.6□□□□□□□□□□□□□□□□□□□“Tab”□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□“Tab”□□□“Enter”□□□□□□□□□□□□□□□□

□□□□□□□□□□ISE□□□□□□□□□□□□□□□□

□□□ □□□PowerShell□□ □□□□□□□□□□□□□□□□□



□2.6 □ISE□□□Tab□□□□□□□□□□□□

2.3 □□□□

□□□□□□□□□□□□□□□□□PowerShell□□□□□□□

- □□□□□□□□□□□□□□——□□□
- 32□ vs 64□——□□□□□64□□Windows□□□64□□PowerShell□□□□□□□□□“x86”□□□□□□□□□□□□□□□□□□□□64□□□□□□64□□Windows□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□32□□□□□□□□□□□64□□□□□□□□□□□□□□□□
- □□PowerShell□□□□□□□□□□□□“□□□”——□□□□□□□□□□□□□“□□□”□□□□□□□□□□□□PowerShell□□□□□“□□□□□□□□”□□□PowerShell□

2.4 □□□□□□□□

□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□“1.0”□□□□□□1.0□□□□Shell□□□□□□□□□□□□□□□□□□v1□□□□PowerShell□□□□□□□□□□□□

```
PS C:\> $PSVersionTable
Name                           Value
----                           ----
PSVersion                      3.0
WSManStackVersion               3.0
SerializationVersion            1.1.0.1
CLRVersion                     4.0.30319.17379
BuildVersion                   6.2.8250.0
PSCompatibleVersions            {1.0, 2.0, 3.0}
PSRemotingProtocolVersion       2.2
```

□□$PSVersionTable□□□□“Enter”□□□□□□□□PowerShell□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□PSVersion 3.0□□□□□□□□□□1□□□□□□□□□□□3.0□□□□

□□□□□□□□□□□□PowerShell□□□□□□□PowerShell□□□□□□□□3.0□□□□□□□□□□□□□□□3.0□□□

2.5 [illegible]

[illegible]

[illegible]PowerShell[illegible]

[illegible]MoreLunches.com[illegible]PowerShell[illegible]

[illegible]PowerShell v3[illegible]

[illegible]ISE[illegible]

1[illegible]

2[illegible]

3[illegible]ISE[illegible]

4[illegible]“'”[illegible]“`”[illegible]“Esc”[illegible]“~”[illegible]

5[illegible][][illegible]<>[illegible]{}[illegible]

[illegible]

2.6 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

- *SAPIEN PrimalScript*[illegible]*PrimalForms*——[illegible] http://primaltools.com[illegible]

- *Idera PowerShell Plus*——[illegible]http://idera.com[illegible]

[illegible]ISE[illegible]PowerShell[illegible]PowerShell Plus[illegible]

2012[illegible]1[illegible]Don[illegible]PowerShell[illegible]2014[illegible]1[illegible]http://ConcentratedTech.com[illegible]PowerShell v3[illegible]Shell[illegible]

[illegible]3[illegible] [illegible]

[illegible]1[illegible]PowerShell[illegible]-CLIs[illegible]command-line interfaces[illegible]PowerShell[illegible]

3.1 [illegible]

[illegible]1[illegible]

[illegible]RTFM[illegible]Read The Friendly Manual[illegible]“[illegible]”[illegible]GUI[illegible]GUI[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]Windows[illegible]Exchange[illegible]GUI[illegible]

[illegible]PowerShell[illegible]

- [illegible]Google[illegible]Bing[illegible]
- [illegible]
- [illegible]Google[illegible]Bing[illegible]

[illegible]90%[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]

[illegible]PowerShell[illegible]

[illegible]

Command[illegible]Cmdlet

PowerShell [illegible]Cmdlet[illegible]Cmdlet [illegible]PowerShell[illegible]Cmdlet[illegible]“[illegible]”[illegible]

3.2 [illegible]

[illegible]

[illegible]PowerShell v3[illegible]“[illegible]”[illegible]PowerShell[illegible]

[illegible]

```
PS C:\> help Get-Service

NAME
    Get-Service

SYNTAX
```

```
    Get-Service [[-Name] <string[]>] [-ComputerName <string[]>]
    [-DependentServices] [-RequiredServices] [-Include <string[]>]
    [-Exclude <string[]>] [<CommonParameters>]

    Get-Service -DisplayName <string[]> [-ComputerName <string[]>]
    [-DependentServices] [-RequiredServices] [-Include <string[]>]
    [-Exclude <string[]>] [<CommonParameters>]

    Get-Service [-ComputerName <string[]>] [-DependentServices]
    [-RequiredServices] [-Include <string[]>] [-Exclude <string[]>]
    [-InputObject <ServiceController[]>] [<CommonParameters>]

□□
    gsv

□□
    Get-Help □□□□□□□□□□□Cmdlet□□□□□□□□□□
    □□□□□□□□□□□□
        -- □□□Update-Help□□□□□□□□□Cmdlet□□□□□□□□
        -- □□□"Get-Help Get-Service -Online"□□□□
    □□□□http://go.microsoft.com/fwlink/?LinkID=113332
        □□□□□□□□□□□□□□
```

□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell □□□□□□□□□□□

　　□□PowerShell□□□□□□□□□□□□□□□□□□□□System32□□□□□□□□□□Shell□□□□□□□□□□□□□PowerShell □□□□□□□□“□□□”□□□□□□□□□□□□□□□□

```
PS C:\> update-help
Update-Help : □□□□□□□□□□□:
'Microsoft.PowerShell.Management□ Microsoft.PowerShell.Utility□
Microsoft.PowerShell.Diagnostics□ Microsoft.PowerShell.Core□
Microsoft.PowerShell.Host□ Microsoft.PowerShell.Security□
Microsoft.WSMan.Management' :
□□□□□□ Windows PowerShell □□□□□ $pshome\Modules □□□□□□□□□□□□□□□□□□
□□□□□□□□□“□□□□□□□□□”□□□□Windows PowerShell□□□□□□□ Update-Help□
□□□□ □:1 □□: 1
+ update-help
+ ~~~~~~~~~~~
     + CategoryInfo          : InvalidOperation: (:) [Update-Help]□
Except
   ion
     + FullyQualifiedErrorId :
UpdatableHelpSystemRequiresElevation□Micros
   oft.PowerShell.Commands.UpdateHelpCommand
```

[illegible]Shell[illegible]Update-Help[illegible]

[illegible]PowerShell [illegible]

[illegible]Save-Help[illegible]Update-Help[illegible]-SourcePath[illegible]

3.3 [illegible]

Windows[illegible]PowerShell [illegible]Get-Help[illegible]Cmdlet[illegible]“Help”[illegible]“Man”[illegible]Get-Help[illegible]Man[illegible]Help[illegible]Cmdlet[illegible]Cmdlet[illegible]

Help[illegible]Get-Help[illegible]More[illegible]Help Get-Content[illegible] Get-Help Get-Content[illegible]Get-Help Get-Content | More[illegible]Help[illegible]

> [illegible] [illegible]Help[illegible]Man[illegible]Help[illegible]

[illegible]Shell[illegible]Ctrl+C[illegible]Shell[illegible]Ctrl+C[illegible]“[illegible]”[illegible]“[illegible]”[illegible]Windows PowerShell ISE[illegible]Ctrl+C[illegible]“[illegible]”[illegible]

> [illegible] [illegible]ISE[illegible]Help[illegible]Man[illegible]

[illegible]

3.4 □□□□□□□

□□□□□□□□□□□□□□Shell□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□Get-Help□□□□Help□□□□□□□□□□□□□□□□□□□-Name□□-Name□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□

```
Help *log*
Help *event*
```

□□□□□□□□□□□□□□□□□□

```
Name                          Category       Module
----                          --------       ------
Clear-EventLog                Cmdlet
Microsoft.PowerShell.M...
Get-EventLog                  Cmdlet
Microsoft.PowerShell.M...
Limit-EventLog                 Cmdlet
Microsoft.PowerShell.M...
New-EventLog                  Cmdlet
Microsoft.PowerShell.M...
Remove-EventLog                Cmdlet
Microsoft.PowerShell.M...
Show-EventLog                  Cmdlet
Microsoft.PowerShell.M...
Write-EventLog                  Cmdlet
Microsoft.PowerShell.M...
Get-AppxLog                    Function        Appx
Get-DtcLog                     Function        MsDtc
Reset-DtcLog                    Function        MsDtc
Set-DtcLog                     Function        MsDtc
Get-LogProperties               Function        PSDiagnostics
Set-LogProperties               Function        PSDiagnostics
```

```
about_Eventlogs               HelpFile
about_Logical_Operators        HelpFile
```

[illegible] [illegible]Appx[illegible]MsDtc[illegible]7[illegible]

[illegible]“[illegible]-[illegible]”[illegible]Cmdlets[illegible]“about”[illegible]“logical”[illegible]“log”[illegible]“*event*”[illegible]“*log*”[illegible]“*eventlog*”[illegible]

[illegible]Cmdlet[illegible]Get-EventLog[illegible]Cmdlet[illegible]

```
Help Get-EventLog
```

[illegible]Tab[illegible]Tab[illegible]Shell[illegible]Tab[illegible]

[illegible]Help Get-Ev[illegible]Tab[illegible]Get-Event[illegible]Tab[illegible]Get-EventLog[illegible]ISE[illegible]Tab[illegible]

[illegible]“*”[illegible]Help[illegible]PowerShell[illegible]

[illegible]Help Get-EventL*[illegible]Get-EventLog[illegible]

[illegible]Get-Eventlog[illegible]

[illegible]

[illegible]Shell[illegible]“[illegible]”[illegible]PowerShell[illegible]

[illegible]Help[illegible]Cmdlet[illegible]Cmdlet[illegible]Get-Command[illegible]Cmdlet[illegible]Gcm[illegible]

[illegible]Help[illegible]Get-Command[illegible]Gcm *event* [illegible]“event”[illegible]Cmdlet[illegible]netevent.dll[illegible]

[illegible]“-[illegible]”[illegible]“-[illegible]”[illegible]Cmdlet[illegible]Cmdlet[illegible]Get-Command -noun *event*[illegible]Get-Command-verb Get[illegible]-CommandType[illegible]Get-Command *log* -type Cmdlet[illegible]“log”[illegible]

3.5 [illegible]

PowerShell[illegible]Cmdlet[illegible]Cmdlet[illegible]

3.5.1 [illegible]

[illegible]Get-EventLog[illegible]

```
SYNTAX
   Get-EventLog [-AsString] [-ComputerName <string[]>] [-List]
[<CommonParameters>]

   Get-EventLog [-LogName] <string> [[-InstanceId] <Int64[]>] [-
After <DateTime>]
   [-AsBaseObject]    [-Before <DateTime>] [-
ComputerName<string[]>] [-EntryType
   <string[]>] [-Index <Int32[]>]    [-Message<string>] [-Newest
```

```
<int>] [-Source
   <string[]>] [-UserName <string[]>]    [<CommonParameters>]
```

[illegible] -
ComputerName [illegible] -
AsString [illegible] -List [illegible]

[illegible] -List [illegible] -AsString [illegible] -
ComputerName [illegible] -List [illegible] -
LogName [illegible] -List [illegible] -LogName [illegible]

[illegible] Shell [illegible]

[illegible] PowerShell [illegible] Cmdlet [illegible]
[<CommonParameters>] [illegible] Cmdlet [illegible] Cmdlet [illegible] 8 [illegible]

[illegible] http://MoreLunches.com [illegible]

3.5.2 [illegible]

[illegible] Cmdlet [illegible] PowerShell [illegible] [-ComputerName <string[]>] [illegible] -ComputerName [illegible] Cmdlet [illegible] [<CommonParameters>] [illegible]

[illegible] Cmdlet [illegible] PowerShell [illegible]

-L -List -L -LogName -Li -List
-Li

Get-EventLog
-LogName
Get-EventLog

Get-EventLog

PowerShell LogName System
Application Ctrl-C

3.5.3

PowerShell

Get-
EventLog

```
[-LogName] <string> [[-InstanceId] <Int64[]>]
```

-LogName
-LogName

-InstanceId
-InstanceId

[illegible]-Before[illegible]Help Get-EventLog[illegible]
[illegible]-Before[illegible]
[illegible]

[illegible]

- [illegible]Get-EventLog -newest 20 -Log Application [illegible]System [illegible]-LogName[illegible]20[illegible]-Newest[illegible]
- [illegible]Get-EventLog-newest 20-Log Application[illegible]-LogName[illegible]-Log[illegible]
- [illegible]Get-EventLog Application 0[illegible]Application[illegible]-LogName[illegible]0[illegible]-InstanceId[illegible]Get-EventLog 0 Application[illegible]0[illegible]-LogName[illegible]“0”[illegible]

[illegible]Cmdlet[illegible]
[illegible]Cmdlet[illegible]
[illegible]

[illegible]

[illegible]Help[illegible]-full[illegible]

[illegible]Help Get-EventLog-full[illegible]Ctrl-C[illegible]

[illegible]-LogName[illegible]

```
-LogName <string>
    [illegible]Log [illegible] LogDisplayName[illegible]
    [illegible]

    [illegible]?                    True
```

```
        □□?                          1
        □□□
        □□□□□□□□?           False
        □□□□□□□?             False
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□

□□□□□□□□□Cmdlet□□□App*□□□□□□□□□□□□□□□□□□Application□

3.5.4 □□□

□□□

```
[-AsString]
```

□□□□□□□□□□□□□□□□□

```
-AsString [<SwitchParameter>]
    □□□□□□□□□□□□□□□□
    □□□□?                 False
    □□?                     named
    □□□
    □□□□□□□□?           False
    □□□□□□□?             False
```

□□[<SwitchParameter>]□□□(□□□□□□□□)□□□□□□□□□□□□□□□□□□□□□□□□

□□□< >:

```
[-LogName] <string>
```

□□□□□□□□□□□□□□□

```
-Message <string>

    [illegible]
    [illegible]?                  False
    [illegible]?                    named
    [illegible]
    [illegible]?            False
    [illegible]?             True
```

[illegible]

- String——[illegible]C:\Windows[illegible]C:\Program Files[illegible]
- Int[illegible]Int32[illegible]or Int64——[illegible]
- DateTime——[illegible]10-10-2010[illegible]-[illegible]-[illegible]

[illegible]

[illegible]

```
[-ComputerName <string[]>]
```

string[illegible]string[][illegible]

```
Get-EventLog Security -computer Server-R2
```

[illegible]PowerShell[illegible]

```
Get-EventLog Security -computer Server-R2[illegible]DC4[illegible]Files02
```

[illegible]

```
Get-EventLog Security -computer 'Server-R2'[illegible]'Files02'
```

[illegible]

```
Get-EventLog Security -computer 'Server-R2[illegible]Files01'
```

[illegible]Cmdlet[illegible]Server-R2[illegible]Files01[illegible]

[illegible]

```
Server-R2
Files02
Files03
DC04
DC03
```

[illegible]Get-Content[illegible]Cmdlet[illegible]-computerName[illegible]Shell[illegible]Get-Content[illegible]

[illegible]PowerShell[illegible]

```
Get-EventLog Application -computer (Get-Content names.txt)
```

[illegible]Web[illegible]

[illegible]Cmdlet[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]Ctrl+C[illegible]

3.5.5 [illegible]

[illegible]PowerShell[illegible]Get-EventLog[illegible]Cmdlet[illegible]

[illegible]Help[illegible]-example[illegible]-full[illegible]

```
Help Get-EventLog -example
```

[illegible]Cmdlet [illegible]

[illegible]

3.6 [illegible]“[illegible]”[illegible]

[illegible]PowerShell[illegible]Cmdlet[illegible]“[illegible]”[illegible]“about_”[illegible]Cmdlet[illegible]

[illegible]

[illegible]“common”[illegible]

```
Help *common*
```

[illegible]About_common _parameters[illegible]8[illegible]

```
-Verbose
-Debug
-WarningAction
-WarningVariable
-ErrorAction
-ErrorVariable
```

```
-OutVariable
-OutBuffer
```

[illegible]“[illegible]”[illegible]Cmdlet[illegible]

[illegible]“[illegible]”[illegible]Cmdlet[illegible]help about*[illegible]Shell[illegible]

[illegible]3.1[illegible]PowerShell[illegible]

[illegible]3.1 PowerShell[illegible]

[illegible]	**URL**
[illegible]PowerShell[illegible]	http://mng.bz/5w8E
[illegible]Widnows[illegible]	http://www.sapien.com/downloads [illegible]“Free Tools”
[illegible]Windows[illegible]“[illegible]”[illegible]PowerShell	http://download.microsoft.com ([illegible])

3.7 [illegible]

PowerShell[illegible]Update-Help[illegible]PowerShell help[illegible]-online[illegible]

```
Help Get-EventLog -online
```

[illegible]TechNet [illegible]PowerShell[illegible]Cmdlet[illegible]PowerShell[illegible]Exchange[illegible]SQLServer[illegible]

[illegible]SharePoint[illegible]PowerShell[illegible]
[illegible]

[illegible]PowerShell[illegible]Web[illegible]Don[illegible]

3.8 [illegible]

> [illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]MoreLunches.com[illegible]

1[illegible]Update-Help[illegible]Shell[illegible]PowerShell[illegible]“[illegible]”[illegible]

2[illegible]Cmdlet[illegible]Cmdlet[illegible]*HTML*[illegible]

3[illegible]Cmdlet[illegible]*file*[illegible]*printer*[illegible]

4[illegible]Cmdlet[illegible]*processes*[illegible]Cmdlet[illegible]

5[illegible]Cmdlet[illegible]*log*[illegible]*write*[illegible]

6[illegible]Cmdlet[illegible]Cmdlet[illegible]*aliases*[illegible]

7[illegible]Shell[illegible]*transcript*[illegible]

8[illegible]*event*[illegible]100[illegible]

9[illegible]*services*[illegible]

10[illegible]*processes*[illegible]

11[illegible]Out-File[illegible]Cmdlet[illegible]Cmdlet[illegible]

12[illegible]Out-File[illegible]Cmdlet[illegible]

13[illegible]PowerShell[illegible]*aliases*[illegible]

14[illegible]Server1[illegible]

15[illegible]Cmdlet[illegible]“object”[illegible]“objects”[illegible]

16[illegible]*arrays*[illegible]

[illegible]4[illegible] [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible].NET Framework[illegible]MVP[illegible]PowerShell[illegible]Geek[illegible]Shell[illegible]

4.1 [illegible]

PowerShell[illegible]Shell[illegible]Cmd.exe[illegible]Shell[illegible]20[illegible]80[illegible]PC[illegible]MS-DOS[illegible]Unix[illegible]Shell[illegible]20[illegible]80[illegible]Bash[illegible]20[illegible]70[illegible]Unix Bourne Shell[illegible]PowerShell[illegible]PowerShell[illegible]VBScript[illegible]KiXtart[illegible]

[illegible]Windows[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible].PS1[illegible]“PowerShell[illegible]”[illegible]Cmd.exe Shell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]VBScript[illegible]PowerShell[illegible].Net Framework[illegible]PowerShell“[illegible]”[illegible]Visual Studio[illegible]C#[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□Jeff□□□□□□□□□Top Gear□□□□□□
BBC□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□

□□□□□□□□□“PowerShell□□”□□□□□□Shell□□
□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□
□□□□□□□□□□□Shell□□□□□

4.2 □□□□□

□4.1□□□□PowerShell□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□

Command | Parameter 1 | Parameter 2 | Parameter 3

```
Get-EventLog -LogName Security -ComputerName WIN8,SERVER1 -Verbose
```

参数名称 | 参数值 | 参数名 | 参数值(多个) | 开关参数(无值)

□4.1 □□□□PowerShell□□

□□□□□□□PowerShell□□□□□□□□□□□□□

- □□Get-EventLog□Cmdlet□PowerShell Cmdlet□□□□□-□□□□□□□□□□Cmdlet□□□□□
- □□□□□-LogName□□□Security□□□□□□□□□□□□□□□□□□□□□
- □□□□□-ComputerName□□□□□□□□□□Win8□Server1□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□-Verbose□□□□□□□□□□□□□□□□□□□□□

- [illegible]
- [illegible]-[illegible]
- [illegible]
- [illegible]
- PowerShell[illegible]

[illegible]PowerShell[illegible]

4.3 Cmdlet[illegible]

[illegible]PowerShell[illegible]

- Cmdlet[illegible]PowerShell[illegible]PowerShell[illegible]C#[illegible].Net Framework[illegible]Cmdlet[illegible]PowerShell[illegible]Google[illegible]Bing[illegible]PowerShell[illegible]“command-let”[illegible]
- [illegible]Cmdlet[illegible].Net[illegible]PowerShell[illegible]
- [illegible]PowerShell[illegible]
- [illegible]PING[illegible]Ipconfig[illegible]
- [illegible]

[illegible]Cmdlet[illegible]

[illegible]Get[illegible]Set[illegible]New[illegible]Pause[illegible]Get-Verb[illegible]100[illegible]

[illegible]Service[illegible]Process[illegible]EventLog[illegible]PowerShell[illegible]“Get-Noun”[illegible]Cmdlet[illegible]

[illegible]Cmdlet[illegible]New-Service[illegible]Get-Service[illegible]Get-Process[illegible]Set-Service[illegible]Exchange[illegible]“Get-Mailbox”[illegible]“Set-User”[illegible]Set-ADUser[illegible]“Get-Command”[illegible]Google[illegible]Bing[illegible]

> [illegible] [illegible]“[illegible]-[illegible]”[illegible]New[illegible]Where[illegible]“[illegible]”[illegible]

4.4 [illegible]

[illegible]PowerShell[illegible]Set-WinDefaultInputMethodOverride[illegible]Tab[illegible]——[illegible]

[illegible]PowerShell[illegible]Get-Service[illegible]

```
PS C:\> get-alias -Definition "Get-Service"
Capability      Name
----------      ----
Cmdlet          gsv -> Get-Service
```

[illegible]Gsv[illegible]Get-Service[illegible]

[illegible]——[illegible]

[illegible]150[illegible]

```
PS C:\> help gsv
NAME
    Get-Service
SYNOPSIS
    Gets the services on a local or remote computer.

SYNTAX
    Get-Service [[-Name] <String[]>] [-ComputerName <String[]>]
    [-DependentServices [<SwitchParameter>]] [-Exclude <String[]>]
    [-Include <String[]>] [-RequiredServices [<SwitchParameter>]]
    [<CommonParameters>]

    Get-Service [-ComputerName <String[]>] [-DependentServices
    [<SwitchParameter>]] [-Exclude <String[]>] [-Include
<String[]>]
    [-RequiredServices [<SwitchParameter>]] -DisplayName
<String[]>
    [<CommonParameters>]

    Get-Service [-ComputerName <String[]>] [-DependentServices
    [<SwitchParameter>]] [-Exclude <String[]>] [-Include
<String[]>]
    [-InputObject <ServiceController[]>] [-RequiredServices
    [<SwitchParameter>]] [<CommonParameters>]
```

[illegible]

[illegible]

[illegible]New-Alias[illegible]Export-Alias[illegible]Shell[illegible]xtd[illegible]xtd[illegible]

4.5 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

□□□

4.5.1 □□□□□□

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□-comp□□-ComputerName□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□-composite□□□□□-computerName□□-common□□□□□□□□-compu□-commo□-compo□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□Tab□□PowerShell□□□□□□□□□□□□□□

4.5.2 □□□□□□

□□□Get-EventLog□□□-ComputerName□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> (get-command get-eventlog | select -ExpandProperty
parameters). Comp
utername.aliases
```

□□-Cn□-computerName □□□□□□□□□□□□□□□□□

```
PS C:\> Get-EventLog -LogName Security -Cn SERVER2 -Newest 10
```

Tab□□□□□□□-Cn□□□□□□□□□□Get-EventLog –C□□□□Tab□□□□□□□□□□□□□□□□□□□□□□□□-Cn□□□□□□□Tab□□□□□□□□-Cn□-ComputerName□□□hi□□□□□□

4.5.3 □□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
SYNTAX
   Get-ChildItem [[-Path] <String[]>] [[-Filter] <String>] [-
```

```
Exclude
    <String[]>] [-Force [<SwitchParameter>]] [-Include <String[]>]
[-Name
   [<SwitchParameter>]] [-Recurse [<SwitchParameter>]] [-
UseTransaction
   [<SwitchParameter>]] [<CommonParameters>]
```

[illegible]-Path[illegible]-Filter[illegible]help Get-ChildItem-Full[illegible]

```
-Path <String[]>
    Specifies a path to one or more locations. Wildcards are
    permitted. The default location is the current directory (.).

    Required?                      false
    Position?                      1
    Default value                  Current directory
    Accept pipeline input?       true (ByValue, ByPropertyName)
    Accept wildcard characters?  True
```

[illegible]-Path[illegible]1[illegible]——[illegible]

```
PS C:\> Get-ChildItem c:\users
    Directory: C:\users
Mode             LastWriteTime   Length  Name
------               --------------    -------  -------
d----         3/27/2012  11:20 AM            donjones
d-r--          2/18/2012   2:06 AM             Public
```

[illegible]

```
PS C:\> Get-ChildItem -path c:\users
    Directory: C:\users
Mode                   LastWriteTime       Length  Name
------               -------------     ------- -------
d----         3/27/2012   11:20 AM               donjones
d-r--         2/18/2012    2:06 AM                 Public
```

[illegible]

[illegible]DIR[illegible]-Path[illegible]3[illegible]4[illegible]

[illegible]

```
PS C:\> move file.txt users\donjones\
```

[illegible]

```
PS C:\> move -Path c:\file.txt -Destination \users\donjones\
```

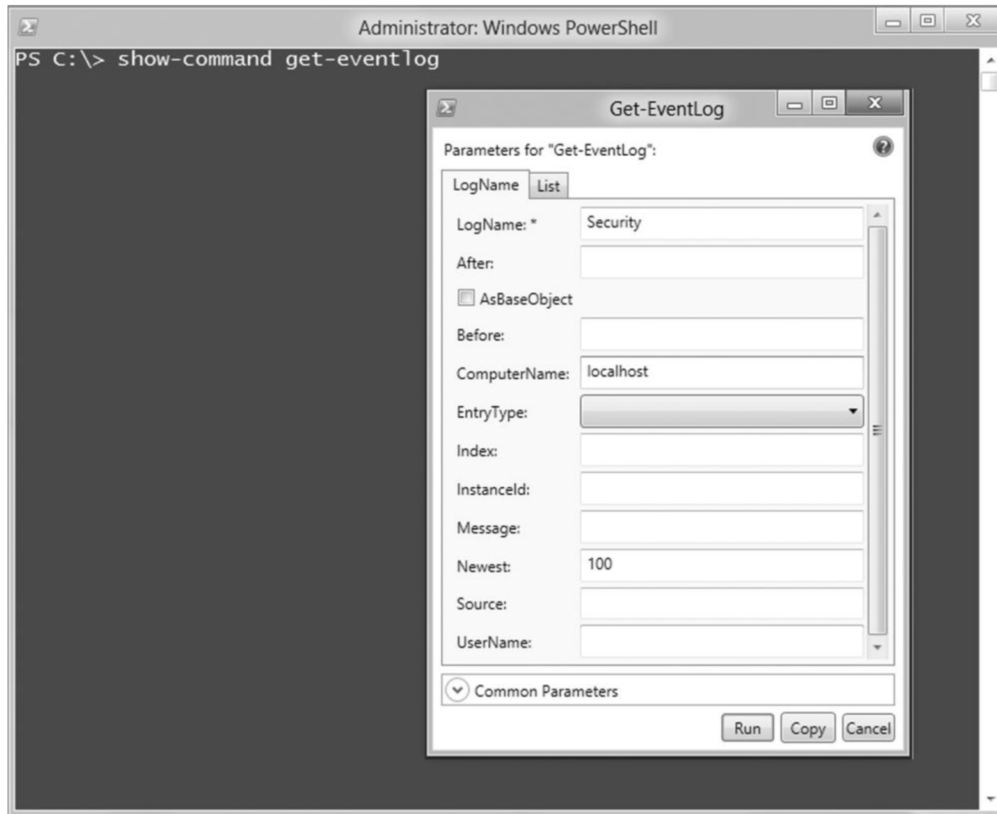
[illegible]

```
PS C:\> move -Destination \users\donjones\ -Path c:\file.txt
```

[illegible]

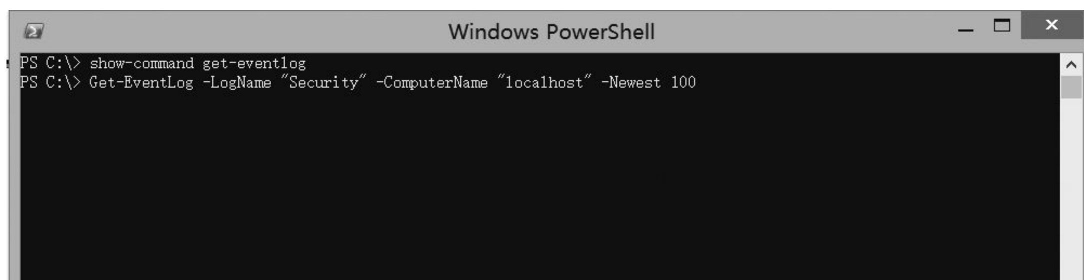
4.6 [illegible]Show-Command

[illegible]PowerShell[illegible]PowerShell v3[illegible]Show-Command commlet[illegible]Show-Command[illegible]4.2[illegible]Tab[illegible]——[illegible]Tab[illegible]



[illegible]4.2 Show-Command[illegible]

[illegible]——[illegible]Shell[illegible]ISE[illegible]Ctrl+V[illegible]Shell[illegible]PowerShell[illegible]4.3[illegible]



[illegible]4.3 [illegible]Show-Command[illegible]

[illegible]PowerShell[illegible]

[illegible]Show-Command[illegible]

4.7 [illegible]

[illegible]Shell[illegible]Cmdlet[illegible]400[illegible]Cmdlet[illegible]Windows[illegible]Windows[illegible]——[illegible]Exchange Server[illegible]Sharepoint Server[illegible]SQL Server[illegible]Cmdlet[illegible]

[illegible]PowerShell[illegible]Cmdlet——[illegible]Ping[illegible]Nslookup[illegible]Ipconfig[illegible]Net[illegible]PowerShell Cmdlet[illegible]PowerShell[illegible]Cmd.exe[illegible]PowerShell[illegible]PowerShell[illegible]CMD[illegible]PowerShell[illegible]——[illegible]Net Use[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]

Net Use[illegible]PowerShell[illegible]“[illegible]”[illegible]“[illegible]”[illegible]PowerShell[illegible]“Map-Drive”[illegible]Net Use[illegible]

> [illegible] [illegible]Net Use[illegible]PowerShell v1[illegible]PowerShell v3[illegible]PowerShell[illegible]New-PSDrive[illegible]-Persisit[illegible]

[illegible]Test-Connection Cmdlet[illegible]Ping[illegible]Ping[illegible]Ping[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]——Shell

[illegible]Shell[illegible]——[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]

```
$exe = "C:\Vmware\vcbMounter.exe"
$host = "server"
$user = "joe"
$password = "password"
$machine = "somepc"
$location = "somelocation"
$backupType = "incremental"

& $exe -h $host -u $user -p $password -s "name:$machine" -r
$location -t
$backupType
```

[illegible]vcbMounter.exe[illegible]VMWare[illegible]——[illegible] 6[illegible]

- -h for the host name
- -u for the user name
- -p for the password
- -s for the server name
- -r for a location
- -t for a backup type

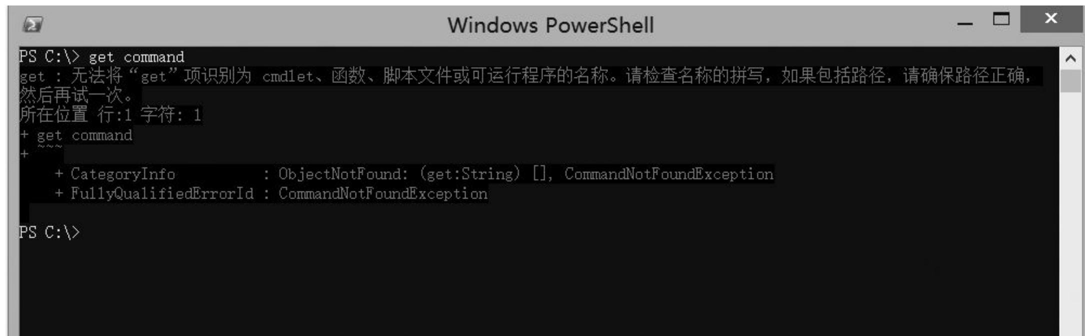
[illegible]——[illegible]$[illegible]PowerShell[illegible]PowerShell[illegible]

□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□Cmd.exe□□□□□□□□□□□Cmd.exe□□□□PowerShell□□□□□□□□□□□□□□□□□□PowerShell□□□

4.8 □□□□

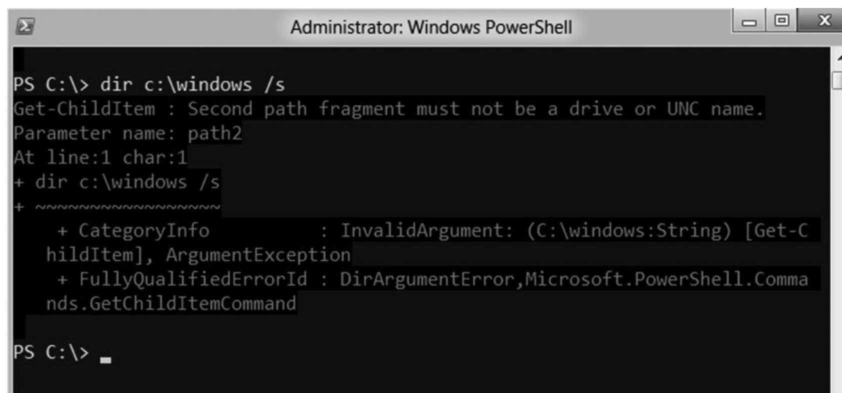
□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□4.4□□□□□□□□□□□PowerShell□□□□□



□4.4 □□PowerShell□□□□□

□□□□□□□□□PowerShell□□□□□□□□□□□□□□4.4□□□□□□□□1——□□□□□□□□□□□□□□“□□□□‘get’□□□□□□□□”□□□□□□□□□□□□□□□Get-Command□□□Get Command□□4.5□□□□?



[illegible]4.5 “[illegible]”[illegible]

[illegible]4.5[illegible]“[illegible]UNC[illegible]”[illegible]c:\windows[illegible]/s[illegible]

[illegible]Get-ChildItem-path C:\Windows[illegible]/s[illegible]-recurse[illegible]PowerShell[illegible]PowerShell[illegible]Show-Command[illegible]

4.9 [illegible]

[illegible]——[illegible]Shell[illegible]

4.9.1 [illegible]Cmdlet[illegible]

[illegible]Cmdlet[illegible]-[illegible]Get-Content[illegible]

- `Get Content`
- `GetContent`
- `Get=Content`
- `Get_Content`

[illegible]“=”[illegible]“-”[illegible]“Get Content”[illegible]

4.9.2 [illegible]

[illegible]-recurse[illegible]Cmdlet[illegible]

- Dir–rec□□□□□□□□□□□□□
- New-PSDrive-name DEMO-psprovider FileSystem-root \\Server\Share□□□□□□□□□
- Dir-rec□□□□□□□□□□□□□□
- New-PSDrive–nameDEMO□□□□□□□□□□□□
- New-PSDrive-name DEMO-psprovider FileSystem□□□□□□□□□□□□□□□□□□□□□□

PowerShell□□□□□□□□□□□□□□□dir□DIR□□□□□-RECURSE□-recurse□-Recurse□□□□□□PowerShell□□□□□□□□□□□□□

4.10 □□□□

□□□ □□□□□□□□□□□□Windows 8□□□□□□□□□Windows 2012□□□□□□□□□□□□□□□□PowerShell□

□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□

1□□□□□□□□□□□□□

2□□□□□□100□□□□□□□□□□□□□Get-WinEvent□□□□□□□□□□□□□□□□□□□□□□□

3□□□□□□□□“Cmdlet”□□□□□□□□□□□Get-Command□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

4□□□□□□□□□

5□□□□□□□□□□□□□□□□□□□□□“D”□□□□□□□

6□□□□□□M□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□*□□□□PowerShell□□□□□□□□

7□□□□□□Windows□□□□□□□□□□Help□Get-Command□□□□□Cmdlet□

8□□□□□Windows□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□

□□□PowerShell□□□

[illegible]5[illegible] [illegible]

PowerShell[illegible]Windows[illegible]Windows[illegible]PowerShell[illegible]Cmd.exe[illegible]

5.1 [illegible]

[illegible]PowerShell[illegible]PSProvider[illegible]Shell[illegible]

```
PS C:\Users\gaizai> Get-PSProvider
Name                  Capabilities           Drives
--------              ----------------         -------
Alias                 ShouldProcess            {Alias}
Environment     ShouldProcess           {Env}
FileSystem     Filter, ShouldProcess, Credentials {C, D, A}
Function      ShouldProcess           {Function}
Registry      ShouldProcess, Transactions    {HKLM, HKCU}
Variable      ShouldProcess           {Variable}
```

[illegible]PowerShell[illegible]PowerShell[illegible]7[illegible]PowerShell[illegible]PSProvider[illegible]13[illegible]PSProvider[illegible]

```
PS C:\Users\gaizai> Get-PSProvider
Name                  Capabilities           Drives
--------             ----------------         -------
Alias                 ShouldProcess            {Alias}
Environment     ShouldProcess           {Env}
FileSystem     Filter, ShouldProcess, Credentials {C, D, A}
Function      ShouldProcess           {Function}
Registry      ShouldProcess, Transactions    {HKLM, HKCU}
Variable      ShouldProcess           {Variable}
WSMan       Credentials              {WSMan}
```

- ShouldProcess—— -WhatIf -Confirm
- Filter—— Cmdlet -Filter
- Credentials—— -Credentials
- Transactions——

PSDrive PSDrive Windows PSDrive PowerShell 3.0

```
PS C:\Users\gaizai> Get-PSDrive
Name   Used (GB)   Free (GB) Provider    Root
------  ---------   --------- --------    ------
A                 FileSystem    A:\
Alias                                    Alias
C     29.40     97.60  FileSystem   C:\
Cert                                      Certificate      \
D     1.26      283.74  FileSystem     D:\
Env                                       Environment
Function                                 Function
HKCU                                      Registry    HKEY_CURRENT_USER
HKLM                                      Registry    HKEY_LOCAL_MACHINE
Variable                                 Variable
WSMan                                    WSMan
```

FileSystem Registry PSProvider PSDrive Cmdlets PSDrive PSDrive Cmdlets “Item” PowerShell 3.0

```
PS C:\Users\gaizai> Get-Command -noun *Item*
CommandType Name   Name
---------------   -------------------
Function      Get-DAEntryPointTableItem   DirectAccessClientComponents
Function      New-DAEntryPointTableItem   DirectAccessClientComponents
Function      Remove-DAEntryPointTableItem
DirectAccessClientComponents
```

```
Function      Rename-DAEntryPointTableItem
DirectAccessClientComponents
Function      Reset-DAEntryPointTableItem  DirectAccessClientComponents
Function      Set-DAEntryPointTableItem   DirectAccessClientComponents
Cmdlet       Clear-Item          Microsoft.PowerShell.Management
Cmdlet       Clear-ItemProperty      Microsoft.PowerShell.Management
Cmdlet       Copy-Item          Microsoft.PowerShell.Management
Cmdlet       Copy-ItemProperty       Microsoft.PowerShell.Management
Cmdlet       Get-ChildItem         Microsoft.PowerShell.Management
Cmdlet       Get-ControlPanelItem     Microsoft.PowerShell.Management
Cmdlet       Get-Item           Microsoft.PowerShell.Management
Cmdlet       Get-ItemProperty       Microsoft.PowerShell.Management
Cmdlet       Invoke-Item         Microsoft.PowerShell.Management
Cmdlet       Move-Item          Microsoft.PowerShell.Management
Cmdlet       Move-ItemProperty       Microsoft.PowerShell.Management
Cmdlet       New-Item           Microsoft.PowerShell.Management
Cmdlet       New-ItemProperty       Microsoft.PowerShell.Management
Cmdlet       Remove-Item         Microsoft.PowerShell.Management
Cmdlet       Remove-ItemProperty      Microsoft.PowerShell.Management
Cmdlet       Rename-Item         Microsoft.PowerShell.Management
Cmdlet       Rename-ItemProperty      Microsoft.PowerShell.Management
Cmdlet       Set-Item           Microsoft.PowerShell.Management
Cmdlet       Set-ItemProperty       Microsoft.PowerShell.Management
Cmdlet       Show-ControlPanelItem     Microsoft.PowerShell.Management
```

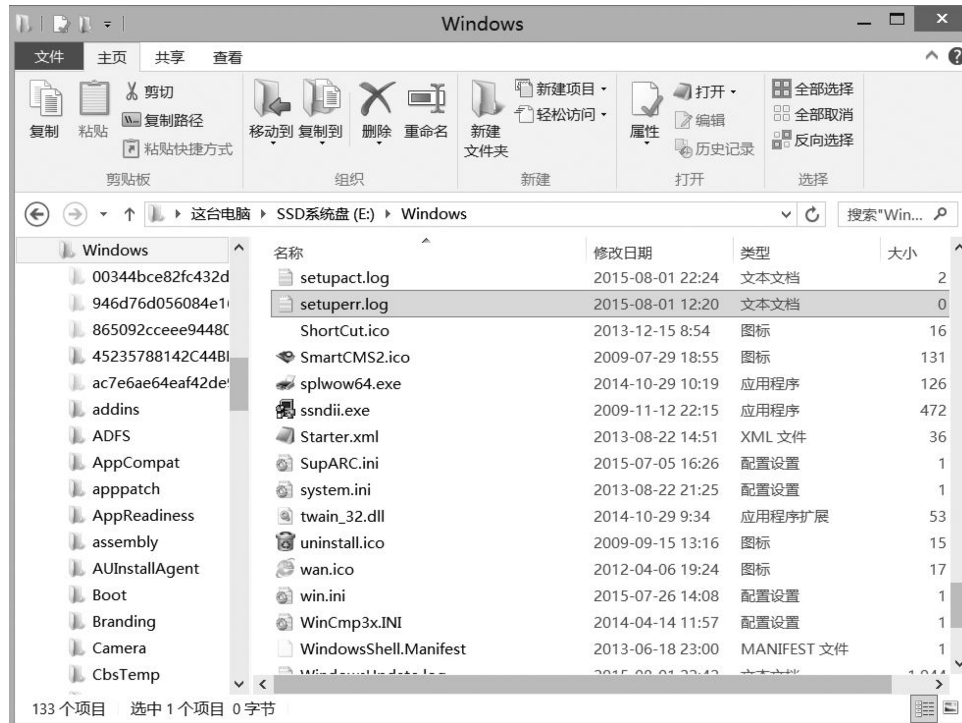
[illegible]Cmdlet[illegible]PSProvider[illegible]

5.2 FileSystem[illegible]

Windows [illegible]

[illegible]Windows[illegible]Windows[illegible]5.1[illegible]

PowerShell[illegible]PSDrive[illegible]——[illegible]PSDrive[illegible]PowerShell[illegible]“[illegible]”[illegible]“[illegible]”[illegible]PowerShell[illegible]“[illegible]”[illegible]Item[illegible]Cmdlet[illegible]“Item”[illegible]



□5.1 □Windows□□□□□□□□□□□□□□□□□□□

□□

- □□Clear□Copy□Get□Move□New□Remove□Rename□□Set□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□
- ItemProperty□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□

□□□□□□Cmdlet□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□FileSystem□□□□□□□□□□□□□Cmdlet□□□□□□-UseTransaction□□□□□□□□Filter□□□□□□□□Cmdlet□□□□□-Filter□□□

□□PSProvider□□□□□□□□□Environment□□PSProvider□□□□□PowerShell□□□ENV□□□□□Env:\PSModulePath□□□□□□□□□□□Windows□□□□□□□□□□□□□□□□

```
PS C:\Users\gaizai> Get-ItemProperty -Path Env:\PSModulePath
Get-ItemProperty : □□□□□□□□□□□□□□□ IPropertyCmdletProvider □□□
□□□□ □:1 □□: 17
```

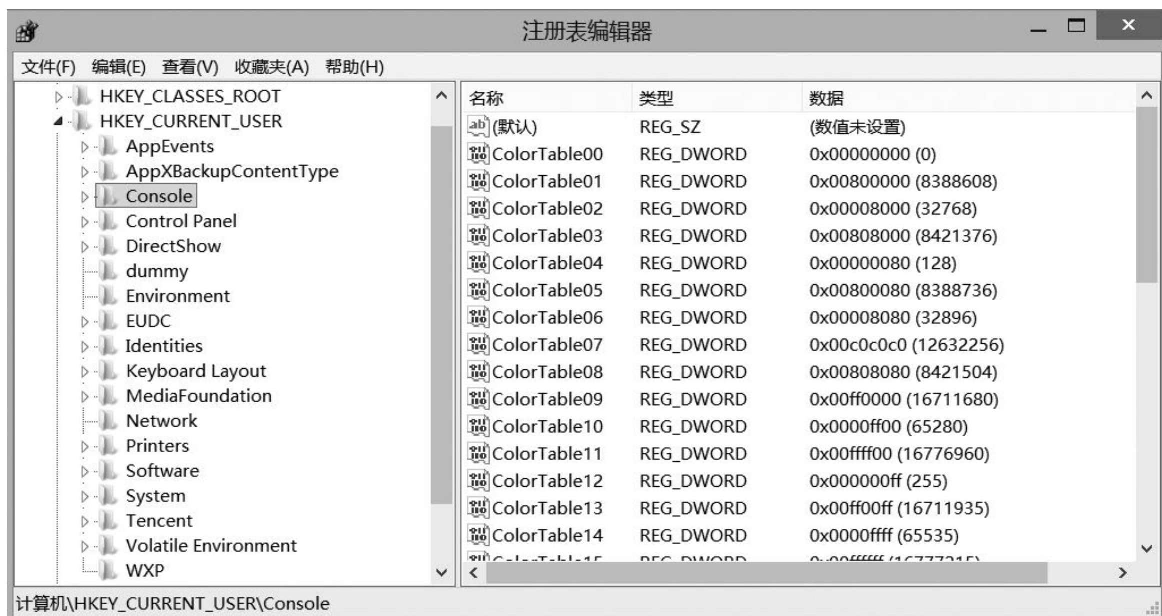
```
+ Get-ItemProperty <<<<  -Path Env:\PSModulePath
    + CategoryInfo      : NotImplemented: (:) [Get-ItemProperty],
PSNotSup
   portedException
    +FullyQualifiedErrorId: NotSupported,
Microsoft.PowerShell.Commands.
   GetItemPropertyCommand
```

[illegible]Windows PowerShell[illegible]PSProvider[illegible]Cmdlet[illegible]

5.3 [illegible]——[illegible]

[illegible]5.2[illegible]Windows[illegible]

[illegible]PowerShell[illegible]Cmdlet[illegible]



[illegible]5.2 [illegible]

5.4 [illegible]

[illegible]Cmdlet[illegible]Set-Location[illegible]Shell[illegible]

```
PS C:\Users\gaizai> Set-Location -Path C:\Windows
PS C:\Windows>
```

[illegible]cd[illegible]cmd.exe[illegible]change directory[illegible]

```
PS C:\Windows> cd 'C:\Program Files'
PS C:\Program Files>
```

[illegible]

PowerShell[illegible]New-Item[illegible]

```
PS C:\Users\gaizai> New-Item testFolder
Type:
```

[illegible]New-Item[illegible]Cmdlet[illegible]——[illegible]Cmdlet[illegible]

```
PS C:\Users\gaizai> New-Item testFolder
Type: Directory

    □□: C:\Users\gaizai
Mode        LastWriteTime    Length  Name
------       --------------  --------   -------
d-----           2015/1/5  14:18       testFolder
```

PowerShell[illegible]MKDir[illegible]New-Item[illegible]MKDir[illegible]

```
PS C:\Users\gaizai> Mkdir test2

    □□: C:\Users\gaizai
Mode       LastWriteTime    Length  Name
-----             ---------------  ------  ------
d-----          2015/1/5   14:22        test2
```

□□□□□□□□Mkdir□□□□□□□□□□□□□□□□□□□□□□□□□□□□New-Item□□□□□□□□□-Type Directory□□□□□□□□□MkDir□□□□□□□Cmd.exe□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

5.5 □□□□□□□□□□□□

□□□□□ Cmdlet□□□□-Path□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-ChildItem□□□□□□□□□□□□□

```
PS C:\Users\gaizai> Get-Help Get-ChildItem –Full
-Path
     □□□□□□□□□□□□□□□□□□□□□□□□□ (.)□

     □□□□?        False
     □□?                  1
     □□□                 Current directory
     □□□□□□□□?     true (ByValue, ByPropertyName)
     □□□□□□□?         True
```

“*”□□□□□0□□□□□□□□“?”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-ChildItem□□□Dir□

```
PS C:\windows> Dir *.exe

     □□: C:\windows

Mode            LastWriteTime      Length  Name
------            --------------      ------  -------
-a---         2012/7/26      3:08       75264  bfsvc.exe
-a---          2013/6/1     11:34      2391280  explorer.exe
-a---         2012/11/6      4:20         883712  HelpPane.exe
-a---         2012/7/26      3:08          17408  hh.exe
-a---         2012/7/26      3:08         159232  regedit.exe
-a---         2012/7/26      3:08         126464  splwow64.exe
-a---         2012/7/26      3:21          10752  winhlp32.exe
-a---         2012/7/26      3:08          10752  write.exe
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□MS-DOS□□□□□□“*”□“?”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“*”□□“?”□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“*”□“?”□□□□□□Item□□□□□□□□□□□□□□□□□□□□□□□□□□□□“?”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“*”□□“?”□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows?

[illegible]Windows?[illegible]“?”[illegible]Windows 7[illegible]Windows 8[illegible]

[illegible]PowerShell[illegible]-LiteralPath[illegible]

```
-LiteralPath
    [illegible] Path [illegible]LiteralPath [illegible]
    [illegible]
    [illegible] Windows PowerShell [illegible]
    [illegible]

    [illegible]?                    True
    [illegible]?                          named
    [illegible]
    [illegible]?             true (ByValue, ByPropertyName)
    [illegible]?              False
```

[illegible]*[illegible]?[illegible]-LiteralPath[illegible]-Path[illegible]-LiteralPath[illegible]-LiteralPath[illegible]*.exe[illegible]-Path[illegible]

5.6 [illegible]

[illegible]Cmdlet[illegible]PSDrive[illegible]PowerShell[illegible]Windows[illegible]Windows[illegible]

[illegible]HKEY_CURRENT_USER[illegible]PowerShell[illegible]HKCU:[illegible]

```
PS C:\windows> Set-Location -Path HKCU:
```

[illegible]

```
PS HKCU:\> Set-Location -Path SoftWare
PS HKCU:\SoftWare> Get-ChildItem

    Hive: HKEY_CURRENT_USER\SoftWare

Name                           Property
----                           --------
AppDataLow
```

```
Microsoft
Mine                          (default) : {}
Policies
Wow6432Node
Classes

PS HKCU:\SoftWare> Set-Location Microsoft
PS HKCU:\SoftWare\Microsoft> Get-ChildItem

    Hive: HKEY_CURRENT_USER\SoftWare\Microsoft

Name                         Property
----                         --------
Active Setup
Advanced INF Setup
Assistance
Command Processor         PathCompletionChar : 9
                             EnableExtensions   : 1
                             CompletionChar      : 9
                           DefaultColor        : 0
CTF
EventSystem
Feeds
FTP                         Use PASV : yes
IME
Internet Connection Wizard  Completed : 1
Internet Explorer
MSF
ServerManager               InitializationComplete        : 1
                              CheckedUnattendLaunchSetting : 1
SystemCertificates
WAB
Windows
Windows NT
Wisp
```

[illegible]Cmdlet[illegible]Cmdlet[illegible]

```
PS HKCU:\SoftWare\Microsoft> Set-Location .\Windows
PS HKCU:\SoftWare\Microsoft\Windows> Get-ChildItem

    Hive: HKEY_CURRENT_USER\SoftWare\Microsoft\Windows

Name                        Property
----                         --------
CurrentVersion
DWM                           Composition                    : 1
                                ColorizationColor            :
3226847725
```

```
                               ColorizationColorBalance     : 87
                                ColorizationAfterglow        :
3226847725
                                ColorizationAfterglowBalance : 10
                                ColorizationBlurBalance      : 3
                                EnableWindowColorization     : 1
                                ColorizationGlassAttribute   : 1
Roaming
Shell
Windows Error Reporting   Disabled              : 0
                               MaxQueueCount          : 50
                                DisableQueue            : 0
                                LoggingDisabled        : 0
                                DontSendAdditionalData  : 0
                                ForceQueue              : 0
                                DontShowUI              : 0
                                ConfigureArchive       : 1
                                MaxArchiveCount        : 500
                                DisableArchive         : 0
                                LastQueuePesterTime     :
130649182874302227
                                LastQueueNoPesterTime   :
130649188485744670
```

□□□□□□□□□□EnableWindowColorization□□□□□□□□□□□0□

```
PS HKCU:\SoftWare\Microsoft\Windows> Set-ItemProperty -Path DWM -
PSPropert Enabl
eWindowColorization -Value 0
```

□□□□□□□□□□□□□□□□□□□□

```
PS HKCU:\SoftWare\Microsoft\Windows> Get-ChildItem

    Hive: HKEY_CURRENT_USER\SoftWare\Microsoft\Windows

Name                        Property
----                        --------
CurrentVersion
DWM                           Composition                    : 1
                               ColorizationColor             :
3226847725
                              ColorizationColorBalance     : 87
                              ColorizationAfterglow         : 3226847725
                              ColorizationAfterglowBalance  : 10
                              ColorizationBlurBalance        : 3
                              EnableWindowColorization      : 0
                              ColorizationGlassAttribute    : 1
Roaming
```

```
Shell
Windows Error Reporting Disabled            : 0
                              MaxQueueCount             : 50
                             DisableQueue              : 0
                              LoggingDisabled          : 0
                             DontSendAdditionalData  : 0
                             ForceQueue                : 0
                            DontShowUI                : 0
                             ConfigureArchive         : 1
                            MaxArchiveCount          : 500
                             DisableArchive            : 0
                             LastQueuePesterTime     :
130649182874302227
                             LastQueueNoPesterTime   :
130649188485744670
```

□□

5.7 □□□□

□□□

> □□□□□□□□□□□□3.0□□□□□□□□PowerShell□

□□□□□□□

1□□□□□□□□□□ HKEY_CURRENT_USER\software\microsoft\Windows \ currentversion\explorer□□□“Advanced”□□□□□DontPrettyPath□□□0□

2□□□□□□C:\Test.txt□□□New-Item□□□□

3□□□□□Set-Item□□□Test.txt□□□□TESTING□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

4□Get-ChildItem□-Filter□-Include□-Exclude□□□□□□□□□□

5.8 □□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□Internet Information Service□IIS□□SQL Server□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□IIS□SQL Server□□□□□□□□□□Cmdlet□□□□□

□□□□□□□□□□□□IIS□□□□□7.5□□□□□□□□□SQL Server□□□□□□SQL Server 2012□□“□□□”□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□

□6□ □□□□□□□

□□4□□□□□□□□PowerShell□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□□“Enter”□□□□PowerShell□□

6.1 □□□□□□□□□□□□□□□□

PowerShell□□□□□pipeline□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□“Dir | More”□□□□□□□□□□“Dir”□□□□□□□□□□□□□□“More”□□□“More”□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□PowerShell□□□□□Unix□Linux□Shell□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□

6.2 □□□□CSV□XML□□

□□□□□□□□□□□□

- Get-Process□□□Ps□
- Get-Service□□□Gsv□
- Get-EventLog Security-newest 100

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Get-Process”□“Get-Service”□□□□□□“Get-EventLog”□□□□□□□□“-newest”□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□“Get-Process”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□“Get-Process”□□□□□□□□□6.1□□□□

```
Windows PowerShell
PS E:\Users\Careyson> get-process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
    161      20     3224       4424   100            2268 AppleMobileDeviceService
     85       6     1396       1348   114            5552 appverif
     85       6     1396       1352   114            5568 appverif
     85       6     1392       1352   114            5584 appverif
     84       9     9072       2672    65            5608 appverif
     72       6      972       2016    17            1844 AsLdrSrv
    155      15     3356       9384    99     0.11   1360 AsusTPCenter
     46       6     1156       4440    50     0.02   6676 AsusTPHelper
    136      11     1940       8480    82     0.06   9008 AsusTPLoader
     65       5      804        840    42            5800 AtBroker
     65       5      792        840    42            5816 AtBroker
     65       5      808        844    42            5840 AtBroker
     65       5      808        852    42            5872 AtBroker
    100      13     2356      10176   114     0.13   3640 ATKOSD2
    166      14    10304      12696    51    93.45   6360 audiodg
    122      10    15628      14924    98            3652 bootim
    122      10    15844      15036    98            5216 bootim
    122      10    15632      15084    98            5576 bootim
    122      10    15716      15060    98            5748 bootim
    116      12     4568       4552    78            5208 calc
    116      12     4584       4580    78            5624 calc
    116      12     4580       4560    78            5704 calc
    116      12     4584       4560    78            5808 calc
     70       8     1424       5936    74     0.03  10296 caller64
     90       7     1248       1456    30            5144 CameraSettingsUIHost
     92       7     1260       1464    30            5212 CameraSettingsUIHost
     91       7     1328       1532    30            5448 CameraSettingsUIHost
     91       7     1248       1468    30            5916 CameraSettingsUIHost
     89       6     1160       1388    30            5280 CertEnrollCtrl
     90       6     1164       1396    30            5892 CertEnrollCtrl
```

□6.1 “Get-Process”□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□CPU□□□□□□□□□□□□□□□□□□□CSV□□□□□□□Excel□

6.2.1 □□□□CSV

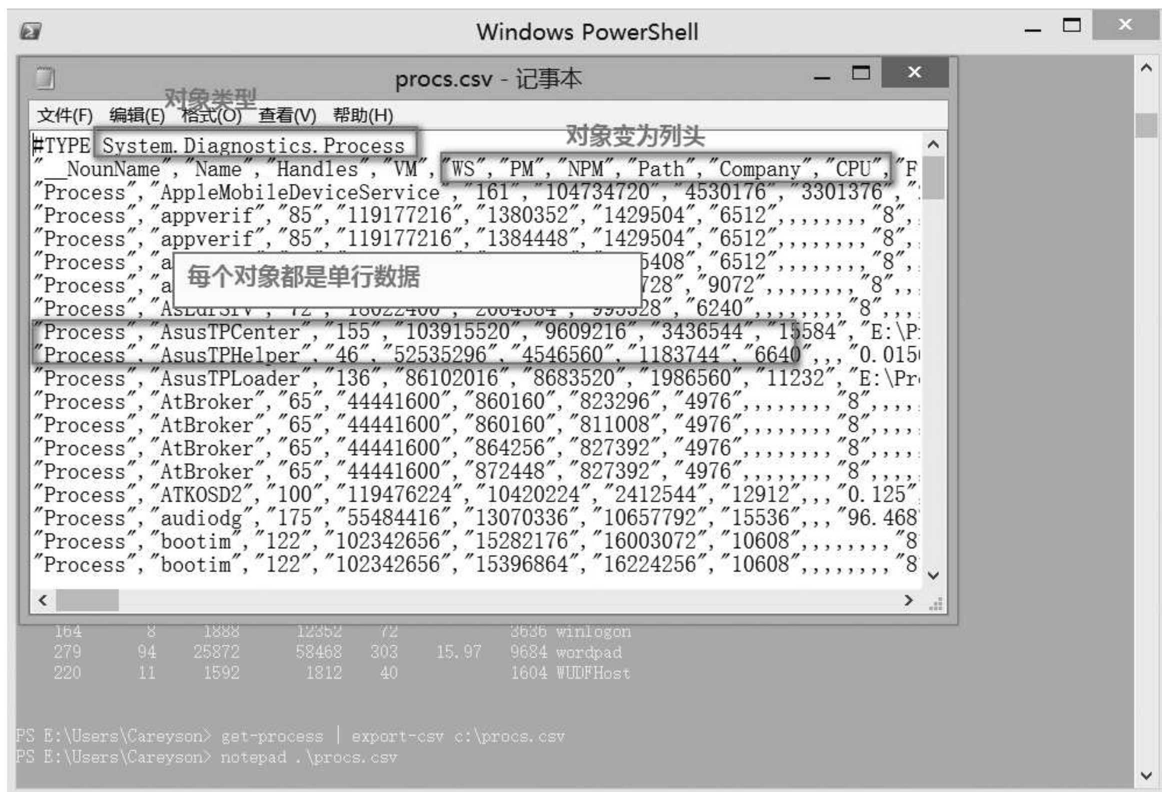
□□□□□□□□□□□□□□□

```
Get-Process | Export-CSV procs.csv
```

□□□□“Dir”□“More”□□□□□□□□“Export-CSV”□□□Cmdlet□□□□□□□□□□□□□□□“Export-CSV”□□□□PowerShell Cmdlet□□□□□□“Get-Process”□□□□□□□□□□CSV□□□

□□Windows□□□□□□6.2□□

```
Notepad procs.csv
```



□6.2 □Windows□□□□□□□□□□CSV□□

□□□□□□□□□“#”□□□□□□□□□□□□□□□□□□□□□□6.2□□□“System.Diagnostics.Process”□Windows□□

□□□□□□□□□“Get-Cmdlet”□□□□□□“Export-CSV”□□□□□□□□□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□Shell□□

□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□

```
Import-CSV procs.csv
```

Shell□□□CSV□□□□□□□□□□□□□□□□□□□□□□□□□□□CSV□□□□□□□

6.2.2 □□□□□XML

[illegible]CSV[illegible]PowerShell[illegible]“Export-CliXML”Cmdlet[illegible]generic command-line interface (CLI) Extensible Markup Language(XML)[illegible]CliXML[illegible]PowerShell[illegible]XML[illegible]“Import-CliXML”Cmdlet[illegible]import[illegible]export[illegible]Cmdlets[illegible]“Import-CSV”[illegible]“Export-CSV”[illegible]

[illegible]CliXML[illegible]IE[illegible]

[illegible]PowerShell[illegible]“Get-Command”Cmdlet[illegible]“-verb”[illegible]“Import”[illegible]“Export”[illegible]

[illegible]PowerShell[illegible]Cmdlets[illegible]Shell[illegible]

6.2.3 [illegible]

[illegible]CSV[illegible]CliXML[illegible]“Compare-Object”[illegible]Diff[illegible]

[illegible]“help diff”[illegible]-ReferenceObject[illegible]-DifferenceObject[illegible]-Property[illegible]

Diff[illegible]“Get-Process”[illegible]

[illegible]CPU[illegible]“Name”[illegible]Diff[illegible]

[illegible]

```
Get-Process | Export-CliXML reference.xml
```

[illegible]CliXML[illegible]CSV[illegible]CliXML[illegible]CSV[illegible]XML[illegible]

```
Diff -reference (Import-CliXML reference.xml)
➡ -difference (Get-Process) -property Name
```

□□□□□□□□□□□□□□□□□□

- □□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□“Import-CliXML”□“Get-Process”□□“Diff”□□□□□□“Import-CLI”□□□□□□□□“-reference”□□□□□“Get-Process”□□□□□“-difference”□□□□□□□□□□□“-referenceObject”□“-differenceObject”□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□“-reference”□“-difference”□□□□□□□□□□□□□□□□□□□□□□□□□□□□“-ref”□“-diff”□□□□□□□□□□
- □□□□□□□□□□□□□Diff□□□□“Name”□□□□□□□□□“-property”□□□□□□□□□□□□□□□□□□□□□□□□□□□□“VM”“CPU”□“PM”□□□□□□□□□□□□□□□□□□□□□□
- □□“<=”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“=>”□□□□□□□□□□□□□□□□□□□□“Diff”□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CliXML□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□

```
PS C:\> diff -reference (import-clixml reference.xml) -difference (get
-process) -property name

name                             SideIndicator
----                              -------------
calc                             =>
mspaint                         =>
notepad                          =>
conhost                          <=
powerShell_ise                 <=
```

□□Cmdlets□□□□□□□□□□□□□□□□□□□□□CliXML□□□

□□□□□□□□□□□□□□“Diff”□□□□□□□□□“-property”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PM/VM□□

[illegible]“Diff”[illegible]Shell[illegible]“Diff”[illegible]PowerShell[illegible]“Diff”[illegible]

> [illegible] [illegible]“Get-Process”“Get-Service”[illegible]“Get-EventLog”[illegible]PowerShell[illegible]Exchange[illegible]SharePoint[illegible]Cmdlet[illegible]Exchange[illegible]SharePoint[illegible]SQL Server[illegible]26[illegible]“[illegible]”[illegible]Cmdlets[illegible]

6.3 [illegible]

[illegible]“Get-Service”[illegible]“Get-Process”[illegible]Cmdlet[illegible]PowerShell[illegible]

```
Dir > DirectoryList.txt
```

[illegible]“>”[illegible]PowerShell[illegible]cmd.exe[illegible]PowerShell[illegible]

```
Dir | Out-File DirectoryList.txt
```

[illegible]“>”[illegible]“Out-File”[illegible]UTF8[illegible]Unicode[illegible]“Out-File”[illegible]80[illegible]PowerShell[illegible]80[illegible]“Out-File”[illegible]80[illegible]

[illegible]

PowerShell[illegible]“Out-Cmdlets”[illegible]“Out-Default”[illegible]“Out-Cmdlets”[illegible]

[illegible]“Dir”[illegible]“Dir | Out-Default”[illegible]“Out-Default”[illegible]“Out-Host”[illegible]

```
Dir | Out-Default | Out-Host
```

[illegible]“Out-Host”[illegible]“Out-Cmdlets”[illegible]

□□□□□□□□□□□□“Out-Cmdlets”□□□□□□□“Help”□□□□□□□□“Help Out*”□□□□□□□□□□□□□□□□□□□□“Get-Command”□□□□“Get-Command Out*”□□□□“-verb”□□□“Get-Command-verb Out”□

“Out-Printer”□□□□□“Out-Cmdlets”□□□□□□□□□□“Out-GridView”□□□□□□□□□□□□□□□□.NET Framework v3.5□Windows PowerShell ISE□□□“Get-Service |Out-GridView”□□□□□“Out-Null”□“Out-String”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

6.4 □□□HTML

□PowerShell□□HTML□□□□□□□□□□□□□□□□□□□□□□“ConvertTo-HTML”□□□□□□□□□□□□□□□□□□□□□HTML□□□□□□□□□Web□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CSS□Cascading Style Sheet□□□□□□□□□□□□□□□□□□□

```
Get-Service | ConvertTo-HTML
```

□□

□PowerShell□□□□□□□“Export”□□□“ConvertTo”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□HTML□□□□□□□□□□□□□□□□□□□□□□□□□HTML□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
Get-Service | ConvertTo-HTML | Out-File services.html
```

□□

PowerShell□□□□“ConvertTo-”Cmdlets□□□□“ConvertTo-CSV”□“ConvertTo-XML”□□□□“ConvertTo-HTML”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CSV□XML□□□□□□□□□□□“Out-File”□□□□□□□□□□□□□□□□□□□□“Export-CSV”□“Export-CliXML”□□□□□□□□□□□□□□□□

[illegible]

[illegible]“Export-CSV”[illegible]“ConvertTo-CSV”[illegible]XML[illegible]

[illegible]XML[illegible]Web[illegible]“ConvertTo-”Cmdlets[illegible]

6.5 [illegible]Cmdlets[illegible]

[illegible]

```
Get-Process | Stop-Process
```

[illegible]Local Security Authority[illegible]PowerShell[illegible]

[illegible]Cmdlets[illegible]

```
Get-Process -name Notepad | Stop-Process
```

[illegible]“Get-Service”[illegible]Cmdlets[illegible]Stop-Service[illegible]Start-Service[illegible]Set-Service[illegible]

[illegible]Get-ADUser | New-SQLDatabase[illegible]7[illegible]

[illegible]“Stop-Service”[illegible]“Stop-Process”[illegible]Cmdlets[illegible]Cmdlets[illegible]impact level[illegible]Cmdlet[illegible]Shell[illegible]“$ConfirmPreference”[illegible]“High”[illegible]Shell[illegible]

```
PS C:\> $ConfirmPreference
High
```

□□□□□□Cmdlet□□□□□□□□□□□Shell□“$ConfirmPreference”□□□□□□Cmdlet□□□□□□□Shell□□□□□□“□□□□□□□□□□Are you sure?□”□□□□□□□□□□□□□□□□□□□□□□“□□”□□□□□□□□□□□□□□□□□□“Are you sure?”□□Cmdlet□□□□□□□□□Shell□“$ConfirmPreference”□□□□□□□□□□□□□□□

□□□□□“□□”□□□□□□□□□□□□□□□□

```
Get-Service | Stop-Service –confirm
```

□□□□□□□“-confirm”□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□

□□□□□□□□□□“-whatif”□□□□□□“-confirm”□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> get-process | stop-process -whatif
What if: Performing operation "Stop-Process" on Target "conhost (1920)
".
What if: Performing operation "Stop-Process" on Target "conhost (1960)
".
What if: Performing operation "Stop-Process" on Target "conhost (2460)
".
What if: Performing operation "Stop-Process" on Target "csrss (316)".
```

□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□

6.6 □□□□

□PowerShell□□□□□□□□□□□□“Export-CSV”□“Export-CliXML”□□□6.2□□□□□□□□□□□□□□□□□□□□□—□□□□□□□□□□□□□□□□XML□

□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□“Get-Content”□□□□□□□□Type/Cat□□□□□□□□□□□□□□□

```
PS C:\> get-eventlog -LogName security -newest 5 | export-csv
events.csv
```

□□□□□□□“Get-Content”□□□Shell□□□□□

```
PS C:\> Get-Content .\events.csv
#TYPE System.Diagnostics.EventLogEntry#security/Microsoft-Windows-
Security
-Auditing/4797
"EventID"□"MachineName"□"Data"□"Index"□"Category"□"CategoryNumber"□"Ent
ryT
ype"□"Message"□"Source"□"ReplacementStrings"□"InstanceId"□"TimeGenerate
d"□
"TimeWritten"□"UserName"□"Site"□"Container"
"4797"□"DONJONES1D96"□"System.Byte[]"□"263"□"
(13824)"□"13824"□"SuccessAudi
t"□"An attempt was made to query the existence of a blank password for
an
account.

Subject:
        Security ID:           S-1-5-21-87969579-3210054174-450162487-
100

        Account Name:           donjones
        Account Domain:        DONJONES1D96
        Logon ID:               0x10526

Additional Information:
        Caller Workstation:     DONJONES1D96
        Target Account Name:    Guest
        Target Account Domain:  DONJONES1D96"□"Microsoft-Windows-
Security-
uditing
"□"System.String[]"□"4797"□"3/29/2012 9:43:36 AM"□"3/29/2012 9:43:36
AM"□□
□
"4616"□"DONJONES1D96"□"System.Byte[]"□"262"□"
(12288)"□"12288"□"SuccessAudi
t"□"The system time was changed.
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Import-CSV”□□□□

```
PS C:\> import-csv .\events.csv

EventID             : 4797
MachineName         : DONJONES1D96
Data                 : System.Byte[]
Index                : 263
Category            : (13824)
CategoryNumber      : 13824
EntryType           : SuccessAudit
Message             : An attempt was made to query the existence of a
```

```
                         blank password for an account.

                         Subject:
                             Security ID:
                         S-1-5-21-87969579-3210054174-450162487-1001
                             Account Name:        donjones
                             Account Domain:        DONJONES1D96
                             Logon ID:        0x10526
                         Additional Information:
                              Caller Workstation:    DONJONES1D96
                              Target Account Name:    Guest
                             Target Account Domain:     DONJONES1D96
Source                : Microsoft-Windows-Security-Auditing
ReplacementStrings : System.String[]
InstanceId            : 4797
TimeGenerated       : 3/29/2012 9:43:36 AM
TimeWritten           : 3/29/2012 9:43:36 AM
UserName              :
```

[illegible]“Import-Cmdlets”[illegible]“Get-EventLog”[illegible]“Export-CSV”[illegible]“Import-CSV”[illegible]“Export-CliXML”[illegible]“Import-CliXML”[illegible]PowerShell[illegible]“Get-Content”[illegible]

6.7 [illegible]

[illegible] [illegible]PowerShell v3[illegible]

[illegible]“[illegible]”[illegible]

1[illegible]“Get-Service | Export-CSV services.csv | Out-File”[illegible]

2[illegible]“Stop-Service”[illegible]“Stop-Service”[illegible]“Get-Service”[illegible]

3[illegible]CSV[illegible]“Export-CSV”[illegible]

4[illegible]CSV[illegible]#[illegible]

5[illegible]“Export-CliXML”[illegible]“Export-CSV”[illegible]

6[illegible]Windows[illegible]“Export-CSV”[illegible]

[illegible]1[illegible]

□7□ □□□□

□□□□□PowerShell□□□□□□□□□□□□□PowerShell□□□□□□□□
Exchange Server□SharePoint Server□System Center□□□SQL
Server□□□Windows
PowerShell□□□□□□□□□□□□

7.1 □□□□□Shell□□□□□□

□□□□□□□□□□□□□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□□
PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□MMC□PowerShell□
□□□□□□□□□□□□□□□

□□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□□□□MMC□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□/□□□□□□□□MMC□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□DNS□□□DHCP□□□□□□□MMC□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□Exchange Server□Forefront□□System
Center□□□□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□□□MMC□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□
□□□□Exchange Server MMC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□MMC□□□□□□□□□□□□□□□□□□

PowerShell□□□□□□□□□□MMC□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□Windows 7□□□□□Exchange Server□□□□□□□□
□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□Shell□□
□□□

7.2 □□□□□“□□Shell”

□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□Windows PowerShell□
□□□□□□Exchange PowerShell□□□□□PowerShell□□□□□Shell□

□□□□□□□□□Windows Server 2008 R2□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows PowerShell□□

```
%windir%\system32\WindowsPowerShell\v1.0\powerShell.exe
➡-noexit -command import-module ActiveDirectory
```

□□□□□□□□PowerShell.exe□□□□□□□□□□□□□□□□□□□□□Import-Module ActiveDirectory□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□”□PowerShell□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□“□□Shell”□Exchange□SharePoint□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell.exe□□□

SQL Server 2008 □SQL Server 2008 R2□□□□□□□“□□□□”Shell□□Sqlps□□□□□□□□□□□□□□□SQL Server□□□PowerShell□□□□□□mini-Shell□□□□□□□SQL Server□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□SQL Server 2012 □□□□PowerShell□

□□□□□□□□□□□□□□□□□□□□Exchange□□□Shell□□□□□□□□Import-Module ActiveDirectory□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□

□□PowerShell□□□□□□□□□□□Don□□□□□□□□□□□□http://windowsitpro.com/go/DonJonesPowerShell□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□Shell□□PowerShell□

7.3 □□□□□□□□□□□

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□PowerShell□□□□PSSnapin□□□□□□□□□□□□□□□□MMS□PSSnapins□PowerShell v1□□□□□□□□□□□□□□PSSnapin□□□□□□□□□DLL□□□□□□□□□□□□□XML□□□□□□□□PSSnapins□□□□□□□□□□□PowerShell□□□□□□□□□



PSSnapin□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□PowerShell□□□Get-PSSnapin -registered□□□□□□□□□□□□□□□□□□□□SQL Server 2008□□□□□□□□□□

```
PS C:\> get-pssnapin -registered

Name         : SqlServerCmdletSnapin100
PSVersion   : 2.0
Description  : This is a PowerShell snap-in that includes various SQL
       Server Cmdlets.
Name         : SqlServerProviderSnapin100
PSVersion   : 2.0
Description  : SQL Server Provider
```

□□□□□□□□□□□□□□□□□□□□□□□□□□Get-PSSnapin□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□

□□□Add-PSSnapin□□□□□□□□□□□□□□

```
PS C:\> add-pssnapin sqlserverCmdletsnapin100
```

□□□PowerShell□□□□□□□□□□□Shell□□□□□

□□□□□□□□□□□□□Shell□□□□□□□PSSnapin□□□Cmdlets□□□PSDrive□□□□□□□Get-Command□□□□Gcm□□□□□□Cmdlets□□

```
PS C:\> gcm -pssnapin sqlserverCmdletsnapin100

CommandType   Name           Definition
-----------   ----           ----------
Cmdlet     Invoke-PolicyEvaluation   Invoke-PolicyEvaluation...
Cmdlet     Invoke-Sqlcmd       Invoke-Sqlcmd [[-Query]...
```

□□□□□□□□□□□□□SqlServerCmdletSnapin100□□□□□□□□□□□□□□SQL Server□□□□□□□□□□□□□□□□Transact-SQL(T-SQL)□□□□□□□T-SQL□□SQL Server□□□□□□□Invoke-Sqlcmd□Cmdlet□□□□□□□□□

□Get-PSProvider□□□□□□□□□□PSDrive□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> get-psprovider

Name      Capabilities       Drives
----      ------------       ------
WSMan      Credentials       {WSMan}
Alias      ShouldProcess      {Alias}
Environment   ShouldProcess      {Env}
FileSystem    Filter, ShouldProcess   {C, A, D}
Function     ShouldProcess      {Function}
Registry     ShouldProcess, Transa... {HKLM, HKCU}
Variable     ShouldProcess      {Variable}
Certificate   ShouldProcess      {cert}
```

[illegible]SqlServer CmdletSnapin100[illegible] SqlServerProviderSnapin100[illegible]Cmdlets[illegible] PSDrive[illegible]

```
PS C:\> add-pssnapin sqlserverprovidersnapin100
PS C:\> get-psprovider

Name      Capabilities       Drives
----      ------------       ------
WSMan      Credentials       {WSMan}
Alias      ShouldProcess      {Alias}
Environment   ShouldProcess      {Env}
FileSystem    Filter, ShouldProcess   {C, A, D}
Function     ShouldProcess      {Function}
Registry     ShouldProcess, Transa... {HKLM, HKCU}
Variable     ShouldProcess      {Variable}
Certificate   ShouldProcess      {cert}
SqlServer    Credentials       {SQLSERVER}
```

[illegible]SQL Server[illegible]Shell[illegible]SQL Server[illegible]PSDrive[illegible]cd SQL server[illegible]SQL Server[illegible]

7.4 [illegible]

PowerShell[illegible]PSSnapins[illegible]

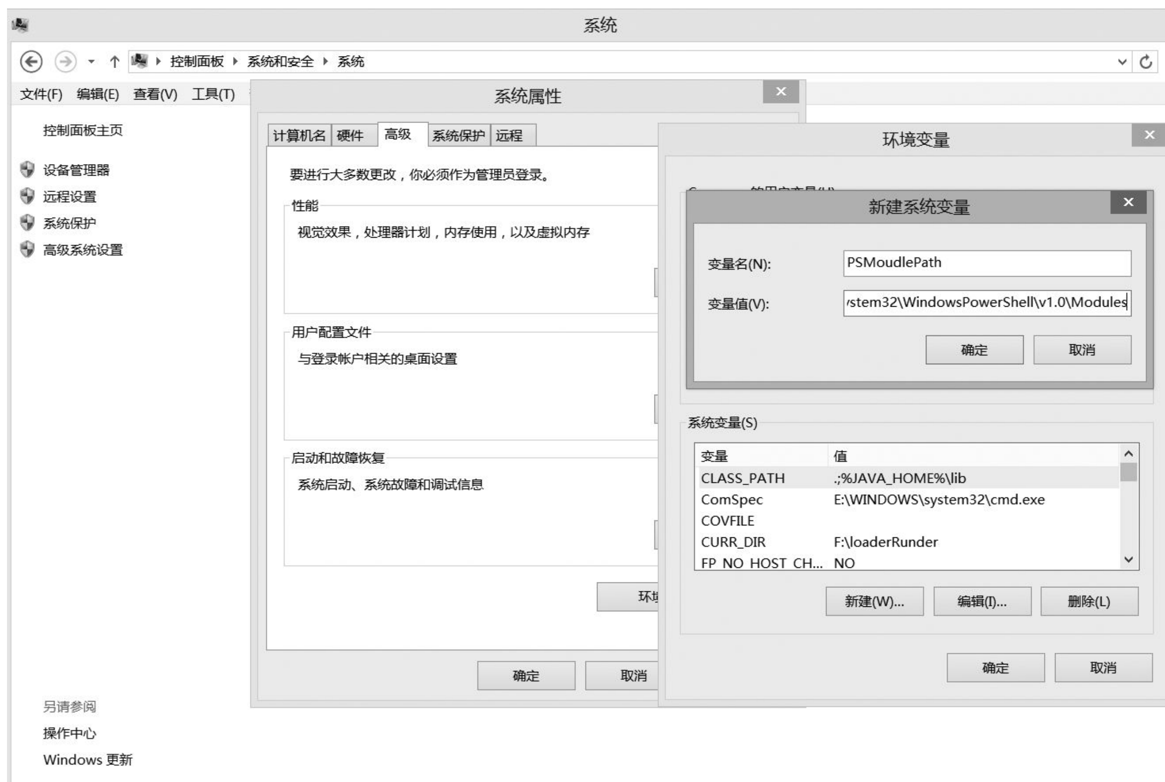
[illegible]PowerShell[illegible] PSModulePath[illegible]PowerShell[illegible]

```
PS C:\> get-content env:psmodulepath
C:\Users\Administrator\Documents\WindowsPowerShell\Modules;C:\Windows
\system32\WindowsPowerShell\v1.0\Modules\
```

□□□

□□□ PSModulePath□□□□PowerShell□□

□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□PSModulePath□□□□□□7.1□□□□□□□□□□□PowerShell□□□□□□□



□7.1 □□Windows□□PSModulePath□□□□

□□□PSModulePath□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□PowerShell□□□PowerShell□□□□□□□□□□□□PowerShell□Update-Help□□□□PSModulePath□□□□□□□□□□□□□□□□□□□□□

[illegible]Get-Module | Remove-Module[illegible]Windows[illegible]

```
PS C:\> help *network*

Name             Category   Module
----             --------   ------
Get-BCNetworkConfiguration   Function   BranchCache
Get-DtcNetworkSetting      Function   MsDtc
Set-DtcNetworkSetting      Function   MsDtc
Get-SmbServerNetworkInterface  Function   SmbShare
Get-SmbClientNetworkInterface  Function   SmbShare
```

[illegible]PowerShell[illegible]"network"[illegible]

```
PS C:\> help Get-SmbServerNetworkInterface

[illegible]
    Get-SmbServerNetworkInterface
[illegible]
    Get-SmbServerNetworkInterface [-CimSession <CimSession[]>]
     [-ThrottleLimit <int>] [-AsJob] [<CommonParameters>]
```

[illegible]PowerShell[illegible]Shell[illegible]

> [illegible] [illegible]Get-Module[illegible]Import-Module[illegible]PowerShell[illegible]13[illegible]

[illegible]PowerShell[illegible]Shell[illegible]Tab[illegible]ISE[illegible]PSModulePath[illegible]

[illegible]PSModulePath[illegible]Import-Module[illegible]C:\MyPrograms\Something\MyModule[illegible]

[illegible]Shell[illegible]Share Point Server[illegible]PowerShell[illegible]Import-Module[illegible]

[illegible]PSDrive[illegible]PSSnapins[illegible]Get-PSProvider[illegible]

7.5 [illegible]

[illegible]SQL Server[illegible]

[illegible]PowerShell[illegible]Exchange Server[illegible]Get-ADUser[illegible]Invoke-SqlCmd[illegible]

[illegible]Get-User[illegible]Cmdlet[illegible]Get-User[illegible]PowerShell[illegible]Get-User[illegible]yCoolPowerShellSnapin[illegible]

```
MyCoolPowerShellSnapin\Get-User
```

[illegible]AD[illegible]SQL[illegible]

[illegible]Remove-PSSnapin[illegible]Remove-Module[illegible]

7.6 [illegible]

[illegible]Windows[illegible]

[illegible]DNS[illegible]PowerShell[illegible]

```
PS C:\> help *dns*

Name             Category    Module
----            --------    ------
dnsn             Alias
Resolve-DnsName        Cmdlet    DnsClient
Clear-DnsClientCache      Function    DnsClient
Get-DnsClient         Function    DnsClient
Get-DnsClientCache       Function    DnsClient
```

```
Get-DnsClientGlobalSetting   Function    DnsClient
Get-DnsClientServerAddress   Function    DnsClient
Register-DnsClient       Function    DnsClient
Set-DnsClient         Function    DnsClient
Set-DnsClientGlobalSetting   Function    DnsClient
Set-DnsClientServerAddress   Function    DnsClient
Add-DnsClientNrptRule      Function    DnsClient
Get-DnsClientNrptPolicy     Function    DnsClient
Get-DnsClientNrptGlobal     Function    DnsClient
Get-DnsClientNrptRule      Function    DnsClient
Remove-DnsClientNrptRule    Function    DnsClient
Set-DnsClientNrptGlobal     Function    DnsClient
Set-DnsClientNrptRule      Function    DnsClient
```

[illegible]DnsClient[illegible]Clear-DnsClientCache[illegible]

[illegible] [illegible]DnsClient[illegible]Windows[illegible]

```
PS C:\> import-module -Name DnsClient
PS C:\> get-command -Module DnsClient

Capability    Name
----------    ----
CIM       Add-DnsClientNrptRule
CIM       Clear-DnsClientCache
CIM       Get-DnsClient
CIM       Get-DnsClientCache
CIM       Get-DnsClientGlobalSetting
CIM       Get-DnsClientNrptGlobal
CIM       Get-DnsClientNrptPolicy
CIM       Get-DnsClientNrptRule
CIM       Get-DnsClientServerAddress
CIM       Register-DnsClient
CIM       Remove-DnsClientNrptRule
CIM       Set-DnsClient
CIM       Set-DnsClientGlobalSetting
CIM       Set-DnsClientNrptGlobal
CIM       Set-DnsClientNrptRule
CIM       Set-DnsClientServerAddress
Cmdlet     Resolve-DnsName
```

[illegible] [illegible]Clear-DnsClientCache[illegible]PowerShell[illegible]DnsClient[illegible]

[illegible]Clear-DnsClientCache[illegible]

```
PS C:\> help Clear-DnsClientCache

□□
    Clear-DnsClientCache
□□
    Clear-DnsClientCache [-CimSession <CimSession[]>] [-ThrottleLimit
    <int>] [-AsJob] [-WhatIf] [-Confirm] [<CommonParameters>]
```

[illegible]

```
PS C:\> Clear-DnsClientCache
```

[illegible]

```
PS C:\> Clear-DnsClientCache -verbose
□□□□: The specified name resolution records cached on this machine will
be removed.
Subsequent name resolutions may return up-to-date information.
```

[illegible]-verbose[illegible]

7.7 [illegible]Shell[illegible]

[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]

[illegible]3[illegible]PSSnapins[illegible]

```
Export-Console c:\myShell.psc
```

[illegible]Shell[illegible]XML[illegible]

[illegible]PowerShell[illegible]

```
%windir%\system32\WindowsPowerShell\v1.0\powerShell.exe
➥-noexit -psconsolefile c:\myShell.psc
```

[illegible]PowerShell[illegible]Shell[illegible]

[illegible] [illegible]PowerShell[illegible]PSModulePath[illegible]PSModulePath[illegible]

[illegible]25[illegible]

1[illegible]WindowsPowerShell[illegible]

2[illegible]profile.ps1[illegible]“profile.ps1”[illegible].txt[illegible].txt[illegible]

3[illegible]Add-PSSnapin[illegible]Import-Module[illegible]

4[illegible]PowerShell[illegible]17[illegible]Set-ExecutionPolicy RemoteSigned[illegible]Shell[illegible]GPO[illegible]

5[illegible]Shell[illegible]profile.ps1[illegible]

[illegible] [illegible]cd \[illegible]Shell[illegible]

7.8 [illegible]

[illegible]PowerShell[illegible]-example[illegible]-full[illegible]

[illegible]
Exchange Server[illegible]400[illegible]Help[illegible] Get-
Command[illegible]

7.9 [illegible]

> **[illegible]** [illegible]Windows 7[illegible]Windows Server 2008 R2[illegible]
> PowerShell v3[illegible]

[illegible]

[illegible]“[illegible]ID”[illegible]
Web[illegible]
http://videotraining.interfacett.com[illegible]“[illegible]”[illegible]

[illegible]PowerShell[illegible]

[illegible]

[illegible]8[illegible] [illegible]

[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]8.2[illegible]8.1[illegible]

8.1 [illegible]

[illegible]PowerShell[illegible]Get-Process[illegible]60[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]Get-Process[illegible]Get-Service[illegible]Get-EventLog[illegible]PowerShell[illegible]Get-Process[illegible]67[illegible]CPU[illegible]ID[illegible]PowerShell[illegible]Shell[illegible]

[illegible]ConvertTo-HTML[illegible]

```
Get-Process | ConvertTo-HTML | Out-File processes.html
```

[illegible]HTML[illegible]

[illegible]

[illegible]

```
Get-Process | ConvertTo-HTML
```

[illegible]

[illegible]PowerShell[illegible]“[illegible]”[illegible]4[illegible]

- [illegible]——[illegible]“[illegible]”[illegible]
- [illegible]——[illegible]“[illegible]”[illegible]ID[illegible]
- [illegible]——[illegible]“[illegible]”[illegible]
- [illegible]——[illegible]“[illegible]”[illegible]

[illegible]4[illegible]

8.2 [illegible]PowerShell[illegible]

PowerShell[illegible]PowerShell[illegible]XML[illegible]

[illegible]Windows[illegible]——[illegible]Windows[illegible]

[illegible]PowerShell[illegible]Get-Process[illegible]

```
PS C:\> get-process
Handles   NPM(K)     PM(K)       WS(K) VM(M)   CPU(s)     Id
ProcessName
-------   ------    -----       -----  -----   ------     --  -----
------
      39        5      1876        4340     52     11.33    1920
conhost
```

```
      31         4       792          2260      22      0.00    2460
conhost
      29         4       828          2284    41      0.25    3192
conhost
    574      12     1864         3896    43     1.30     316 csrss
    181       13     5892          6348     59      9.14     356
csrss
    306      29   13936         18312   139      4.36    1300 dfsrs
    125       15     2528         6048    37      0.17    1756
dfssvc
   5159     7329    85052        86436   118      1.80    1356 dns
```

[illegible]Conhost[illegible]Unix[illegible]Linux Shell[illegible]Grep[illegible]“[illegible]58[illegible]64[illegible]‘conhost’[illegible]”[illegible]

```
Handles NPM(K)  PM(K)   WS(K) VM(M)    CPU(s)    Id  ProcessName
------- ------   -----   ----- -----    ------    --  -----------
    39      5     1876     4340    52    11.33  1920  conhost
    31      4      792      2260    22     0.00  2460  conhost
    29        4      828      2284    41     0.25  3192  conhost
```

[illegible]ID[illegible]“[illegible]52[illegible]56[illegible]”[illegible]

```
1920
2460
3192
```

[illegible]ID[illegible]

[illegible]Unix[illegible]Linux[illegible]Grep[illegible]Awk[illegible]Sed[illegible]Unix[illegible]Linux[illegible]Perl[illegible]

[illegible]

- [illegible]

- [illegible]——[illegible]ProcessName[illegible]——[illegible]
- [illegible]

PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]Shell[illegible]

8.3 [illegible]Get-Member

[illegible]PowerShell[illegible]Help[illegible]

[illegible]“[illegible]”[illegible]Get-Member[illegible]Gm[illegible]

[illegible]Gm[illegible]Get-Process[illegible]Gm[illegible]

```
Get-Process | Gm
```

[illegible]Cmdlet[illegible]Get-Process[illegible]PowerShell[illegible]89[illegible]Gm[illegible]Gm[illegible]

```
PS C:\> get-process | gm

   TypeName: System.Diagnostics.Process
Name                          MemberType     Definition
----                        ----------       ----------
```

```
Handles                  AliasProperty   Handles = Handlecount
Name                      AliasProperty   Name = ProcessName
NPM                        AliasProperty   NPM =
NonpagedSystemMemo...
PM                         AliasProperty   PM = PagedMemorySize
VM                           AliasProperty   VM = VirtualMemorySize
WS                           AliasProperty   WS = WorkingSet
Disposed                    Event           System.EventHandler
Disp...
ErrorDataReceived         Event
System.Diagnostics.DataR...
Exited                       Event           System.EventHandler
Exit...
OutputDataReceived        Event
System.Diagnostics.DataR...
BeginErrorReadLine        Method          System.Void
BeginErrorRe...
BeginOutputReadLine     Method          System.Void BeginOutputR...
CancelErrorRead           Method          System.Void
CancelErrorR...
CancelOutputRead           Method          System.Void
CancelOutput...
```

[illegible]

[illegible]

[illegible]Get-Member[illegible]PowerShell[illegible]Cmdlet[illegible]Get-Member[illegible]“Get-Members”[illegible]

[illegible]Get-Member[illegible]TypeName[illegible]—[illegible]

8.4 [illegible]“[illegible]”

[illegible]Gm[illegible]

- [illegible]

- □□□
- NoteProperty□
- □□□□□

□□□□

□□□□□.Net Framework□□□□—□□□□□PowerShell□□□□□—□□□“□□”□PowerShell□□□□□□□□□□ScriptProperty□NoteProperty□AliasProperty□□□□□□□□□□□MSDN□□□□□□□□□□□□□□□□□□□□□□□□□MSDN□□□□□□□□□□□□□□□□□□□

PowerShell□□□□□□□□□□ETS□□□ProcessName□□□□□□□Name□□

□□□PowerShell□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□“□□”□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□ID□□□□1234□□□□□□□□□□□□□NotePad□□□□□□□□□□□□□□□□□□□□□□□□ID□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□Name□□□□□□□□□□□□□□□□□□□□□□□□Name□□□□□□□□□□□□□□□□□PowerShell□90%□□□□□□□□□□□□□

8.5 □□□□□□□□□□□“□□”

□□□Kill□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlets□□□□□

□□Kill□□□□□□□□□□□□□□Cmdlets□

```
Get-Process -Name Notepad | Stop-Process
```

□□□□□□□□Cmdlet□□□□□□□

```
Stop-Process -name Notepad
```

□□□□□□□□□□□□□□PowerShell Cmdlet□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□.NET Framework□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□—□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□□□□Cmdlet□□□□□□□□□GUI□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“PowerShell□□□”□□□□□□□□□□□

□□□□

□□□PowerShell□□Exited□□

8.6 □□□□

□□□PowerShell Cmdlets□□

□□□□□□□□□□□□□□□□□□□□□□□□□□Vitrual Memory□VM□□□□□□□□□□□□□□□□□□□□VM□□□□□□□□□□□□PowerShell□□□□□□□□Cmdlet□Sort-Object□□□□□□□□□□□□□□□□□□□

```
Get-Process | Sort-Object -property VM
```

□□□□□ □□

□□□□□□□□□□□□□□□□□□□□VM□□□□□□□□□□□□□□□□□□□□□□□□□□Sort-Object□□□□□-descending□□□□□□□□□□□□□□□□-property□□

[illegible]Sort-Object[illegible]Sort[illegible]

```
Get-Process | Sort VM –desc
```

[illegible]-descending[illegible]-desc[illegible]-property[illegible]

[illegible]ID[illegible]

```
Get-Process | Sort VM,ID –desc
```

[illegible]

8.7 [illegible]

[illegible]Cmdlet[illegible]Select-Object[illegible]Cmdlet[illegible]PowerShell[illegible]HTML[illegible]ConvertTo-HTML[illegible]Cmdlet[illegible]

[illegible]

```
Get-Process | ConvertTo-HTML | Out-File test1.html
Get-Process | Select-Object -property Name,ID,VM,PM |
➥ConvertTo-HTML | Out-File test2.html
```

[illegible] [illegible]IE[illegible]HTML[illegible]

[illegible]Select-Object[illegible]Select[illegible]-property[illegible]

```
Get-Process | Select Name,ID,VM,PM | ConvertTo-HTML | Out-File
test3.html
```

[illegible]Select-Object[illegible]

```
Get-Process | Select Name，ID，VM，PM
```

[illegible]PowerShell[illegible]

[illegible]

Select-Object[illegible]-First[illegible]-Last[illegible]Get-Process | Select First 10 [illegible]10[illegible]10[illegible]

[illegible] [illegible]Select-Object[illegible]Where-Object[illegible]PowerShell[illegible]Where-Object[illegible]Select-Object[illegible]-First[illegible]-Last[illegible]Where-object[illegible]

8.8 [illegible]

PowerShell[illegible]PowerShell[illegible]

[illegible]

[illegible]

```
Get-Process |
Sort-Object VM -descending |
Out-File c:\procs.txt
```

[illegible]Get-Process[illegible]Sort-Object[illegible]Sort-Object[illegible]Out-File[illegible]PowerShell[illegible]—[illegible]PowerShell[illegible]

□□□□□□□□□□□□□

```
Get-Process |
Sort-Object VM -descending |
Select-Object Name□ID□VM
```

□□□□□□□□□□□□Get-Process□□□□□□□□□□□□□□□Sort-Object□□□□□□□□□□□□□□□□□□Select-Object□□□□□□□□□□□□□□□□□□□□□Select-Object□□□Select-Object□□□□□□□□□□□□□PSObject□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□ □□□□□□□□□□□□□3□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-Process□□□□□□□□□□

□PowerShell□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□PSObject□□□□□□□□□□□□□□□□□□□□□□□□□PSObjects□□□□□□□□□□□□□□PSObjects□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□3□□□□□□□□□□□□Get-Process□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□

□□□□□Gm□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□Gm□

```
Get-Process | Sort VM -descending | gm
Get-Process | Sort VM -descending | Select Name□ID□VM | gm
```

□□□□□ □□□□□□□□□□□□□□□□□□□□□□□

□□□□PowerShell□□□□□□□□□□□□□□□□Gm□□□□□□□□□□□□□□□□□□□□□□System.Diagnostics.Process□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□□□”□□□□□□3□□□□□—Name□ID□VM□□□□□□□□□□□□□□□□

□□Gm□□□□□□□□□□□□□□□□Gm□□□□□□□□□□□□□□□□□“□□□□”□□□□□□□□□Gm□□□□□□□□Microsoft.PowerShell.Commands.
MemberDefinition□□□□□□□□□□□Gm□□□□□□□□□Gm□□□□□

```
Get-Process | Gm | Gm
```

[illegible] [illegible]Get-Process[illegible]Gm[illegible]MemberDefinition[illegible]Gm[illegible]MemberDefinition[illegible]

[illegible]PowerShell[illegible]Gm[illegible]

8.9 [illegible]

[illegible]PowerShell[illegible]

- [illegible]PowerShell[illegible]Gm[illegible]Get-Member[illegible]
- [illegible]Gm[illegible]Get-Process -name Notepad | Stop-Process[illegible]|Gm[illegible]
- [illegible]Get-Process | Gm[illegible]Get-Process|Gm[illegible]
- [illegible]

8.10 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]MoreLunches.com[illegible]

1[illegible]Cmdlet[illegible]

2[illegible]Cmdlet[illegible]

3[illegible]#2[illegible]Cmdlet[illegible]?[illegible]Cmdlet[illegible]

4[illegible]#2[illegible]Cmdlet[illegible]Select-Object[illegible]PowerShell[illegible]

```
DayOfWeek
---------
   Monday
```

5[illegible]hotfix[illegible]Cmdlet[illegible]

6[illegible]#5[illegible]Cmdlet[illegible]ID[illegible]——[illegible]

7[illegible]#6[illegible]ID[illegible]HTML[illegible]

8[illegible]50[illegible]HTML[illegible]Select-Object[illegible]-first[illegible]-last[illegible]Get-Winevent[illegible]Cmdlet[illegible]

[illegible]9[illegible] [illegible]

[illegible]PowerShell[illegible]Get-Process | Sort VM-desc | ConvertTo-HTML | Out-File process.html[illegible]PowerShell[illegible]

9.1 [illegible]

[illegible]PowerShell[illegible]VBScript[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]VBScript[illegible]PowerShell[illegible]

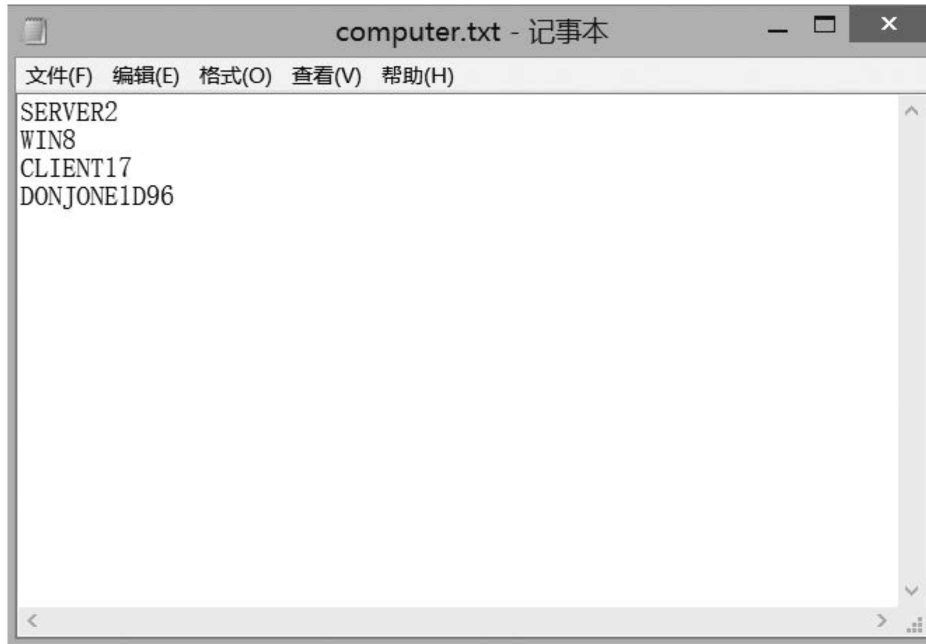
[illegible]Shell[illegible]Shell[illegible]

9.2 PowerShell[illegible]

[illegible]PowerShell[illegible]A[illegible]B[illegible]A[illegible]

```
PS C:\>CommandA | CommandB
```

[illegible]9.1[illegible]



□9.1 □□□□□□□□□□□□□□□□□□□□□□□□□□

□□□

```
PS C:\> Get-Content .\computers.txt | Get-Service
```

□□□Get-Content□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□Get-Service□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□Get-Service□□□□□□□□Get-Content□□□□□□□□□□□□□□□□□□□□□□□Pipeline parameter binding□□□□□□□□□□□□□□□PowerShell□□□□□□□□□Get-Content□□□□□□□□Get-Service□□□□□□□Shell□□□□□□□□□□□□ByValue□□□□□□□□□□□□□□□□ByPropertyName□

9.3 □□A□□□ByValue□□□□□□

□□□ByValue□□□□□□□□□□□□□□PowerShell□□□□□A□□□□□□□□□□□□□□□□□B□□A□□□□□□□□Get-Member□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□B□□□□□□□□□□Help Get-Service -Full□□□□□□B□□□□□□□□□ByValue□□□□□□□□□□9.2□□□□□□□

□□□□□Get-Content□□□□□□□□□□□□□System.String□□□□□□String□□□□□□□□□□□□□□□Get-Service□□□□□□□□□ByValue□□□□□

String[illegible]String[illegible]-Name[illegible]“[illegible]”[illegible]——[illegible]String[illegible]SERVER2[illegible]WIN8[illegible]

```
PS C:\> Get-Content .\computers.txt | Get-Service
```

```
PS C:\>  Get-Content .\computers.txt |

 TypeName:System.String

Name              MemberType
----              ----------
Clone             Method
CompareTo         Method
Contains          Method
CopyTo            Method
EndsWith          Method
Equals            Method
GetEnumerator     Method
GetHashCode       Method
GetType           Method
GetTypeCode       Method
IndexOf           Method
IndexOfAny        Method
Insert            Method
IsNormalized      Method
LastIndexOf       Method
LastIndexOfAny    Method
Normalize         Method
PadLeft           Method
PadRight          Method
Remove            Method
Replace           Method
Split             Method
StartsWith        Method
```

```
Windows PowerShell

    是否必需?                    False
    位置?                        已命名
    是否接受管道输入?            False
    参数集名称           (所有)
    别名                     无
    动态?                    false

-InputObject <ServiceController[]>

    是否必需?                    False
    位置?                        已命名
    是否接受管道输入?            True (ByValue)
    参数集名称           InputObject
    别名                     无
    动态?                    false

-Name <string[]>

    是否必需?                    False
    位置?                        0
    是否接受管道输入?            True (ByValue, ByPropertyName)
    参数集名称           Default
    别名                     ServiceName
    动态?                    false

-RequiredServices

    是否必需?                    False
    位置?                        已命名
```



[illegible]9.2 [illegible]Get-Content[illegible]Get-Service[illegible]

PowerShell[illegible]ByValue[illegible]-Name[illegible]ByValue[illegible]String[illegible]Get-Service[illegible]

[illegible]

```
PS C:\>Get-Process -Name note* | Stop-Process
```

[illegible]A[illegible]Get-Member[illegible]B[illegible]9.3[illegible]

```
PS C:\> get-process -name * | get-member

   TypeName:System.Diagnostics.Process

Name                        MemberType
----                        ----------
Handles                     AliasProperty
Name                        AliasProperty
NPM                         AliasProperty
PM                          AliasProperty
VM                          AliasProperty
WS                          AliasProperty
Disposed                    Event
ErrorDataReceived           Event
Exited                      Event
OutputDataReceived          Event
BeginErrorReadLine          Method
BeginOutputReadLine         Method
CancelErrorRead             Method
CancelOutputRead            Method
Close                       Method
CloseMainWindow             Method
CreateObjRef                Method
Dispose                     Method
Equals                      Method
GetHashCode                 Method
GetLifetimeService          Method
GetType                     Method
InitializeLifetimeService   Method
Kill                        Method
Refresh                     Method
Start                       Method
ToString                    Method
WaitForExit                 Method
WaitForInputIdle            Method
  NounName                  NoteProperty
```

```
Windows PowerShell

    是否必需?                    True
    位置?                        已命名
    是否接受管道输入?            True (ByPropertyName)
    参数集名称         IdWithUserName, Id
    别名                    PID
    动态?                   false

-IncludeUserName

    是否必需?                    True
    位置?                        已命名
    是否接受管道输入?            False
    参数集名称         InputObjectWithUserName, IdWithUserName, NameWithUserName
    别名                    无
    动态?                   false

-InputObject <Process[]>

    是否必需?                    True
    位置?                        已命名
    是否接受管道输入?            True (ByValue)
    参数集名称         InputObjectWithUserName, InputObject
    别名                    无
    动态?                   false

-Module

    是否必需?                    False
    位置?                        已命名
    是否接受管道输入?            False
    参数集名称         InputObject, Id, Name
    别名                    无
    动态?                   false

-Name <string[]>
```

□9.3 □Get-Process□□□□□□□Stop-Service□□□□□□□

Get-Process□□□□□□□□System.Diasnostics.Process□□□□□□□□□□□□□□□□□□□□Process□□□□□□□note□□□□□□□□□□□□NotePad□□□□□□□□□□□□□□□□□□□□□□Stop-Process□□□□□-InputObject□□□□□□□□ByValue□□□□□□□□□□□□□□□□□□□□□“□□□□□□□□□□□□□□□”□□□□□□□A□□□□□□□□□□□□□□□□B□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ByValue□□□□□□□□□□□□□□□Get-Process□Stop-Process□□

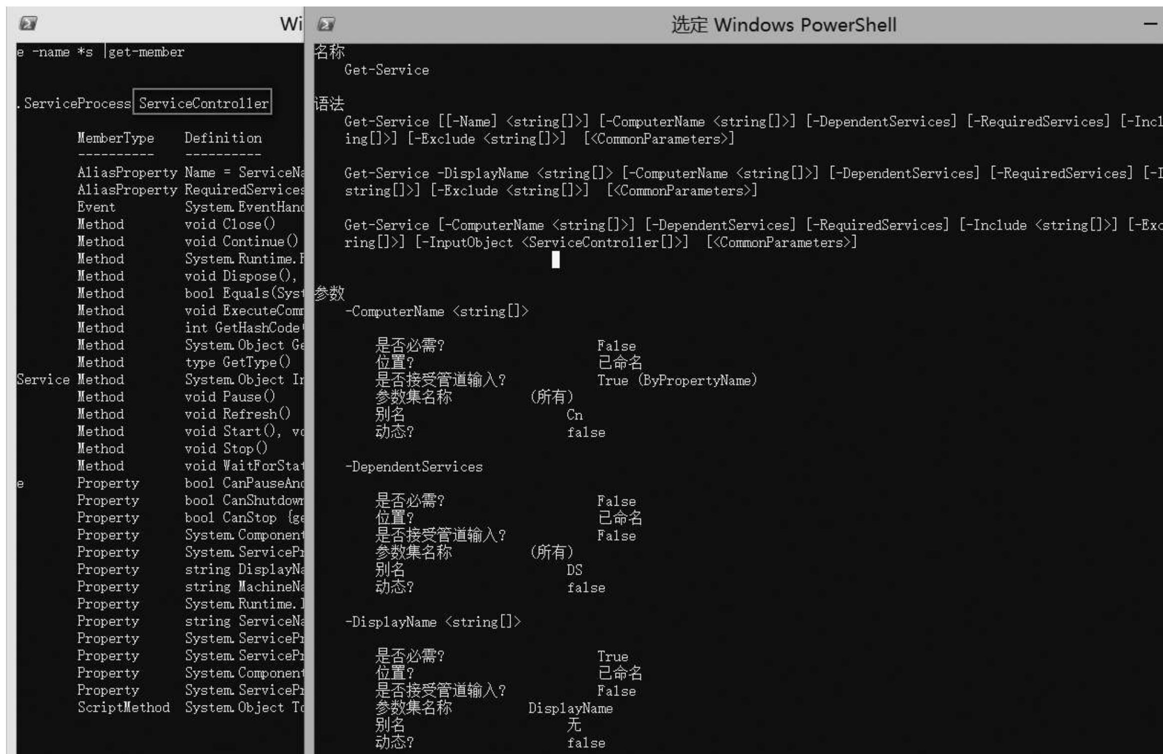
□□□□□□□□□□□□□

```
PS C:\>Get-Service -Name s* | Stop-Process
```

□□□□□□□□□□□□□□□□□□□□□□□□□□A□□□□□□□□□□□Get-Member□□□□□□□B□□□□□□□□□□□□□□9.4□□

Get-Service□□□ServiceController□□□□□□□□□□□□□□System.ServiceProcess. ServiceController□□□□□□□□□□□□□□□□□□□□□□□□□□□Stop-Process□□□□□□□□□□ServiceController□□□□□□□□□□

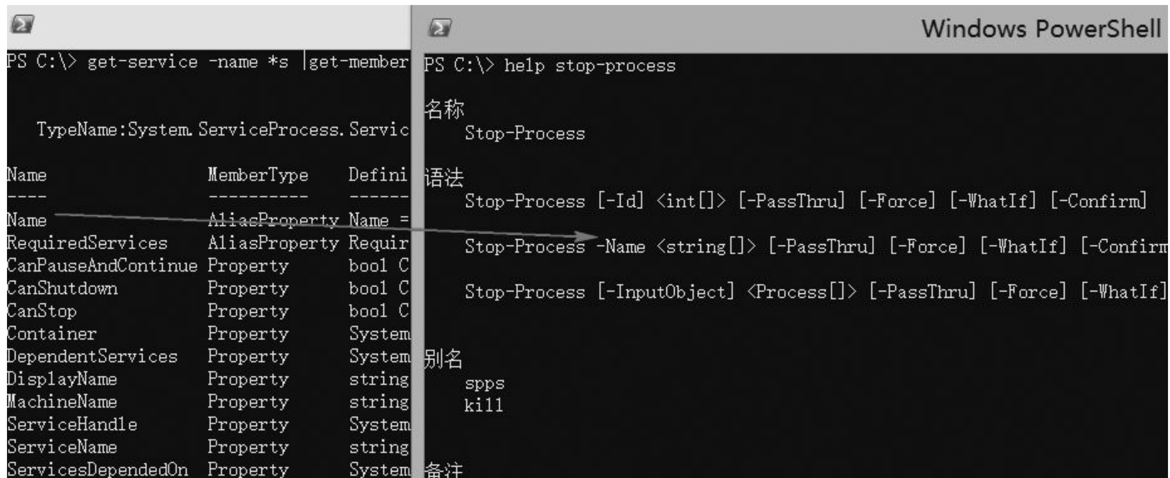
□□□□□ByValue□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□
ByPropertyName□



□9.4 □□Get-Process□□□□□□□Stop-Process□□□□□

9.4 □□B□□□ByPropertyName□□□□□□

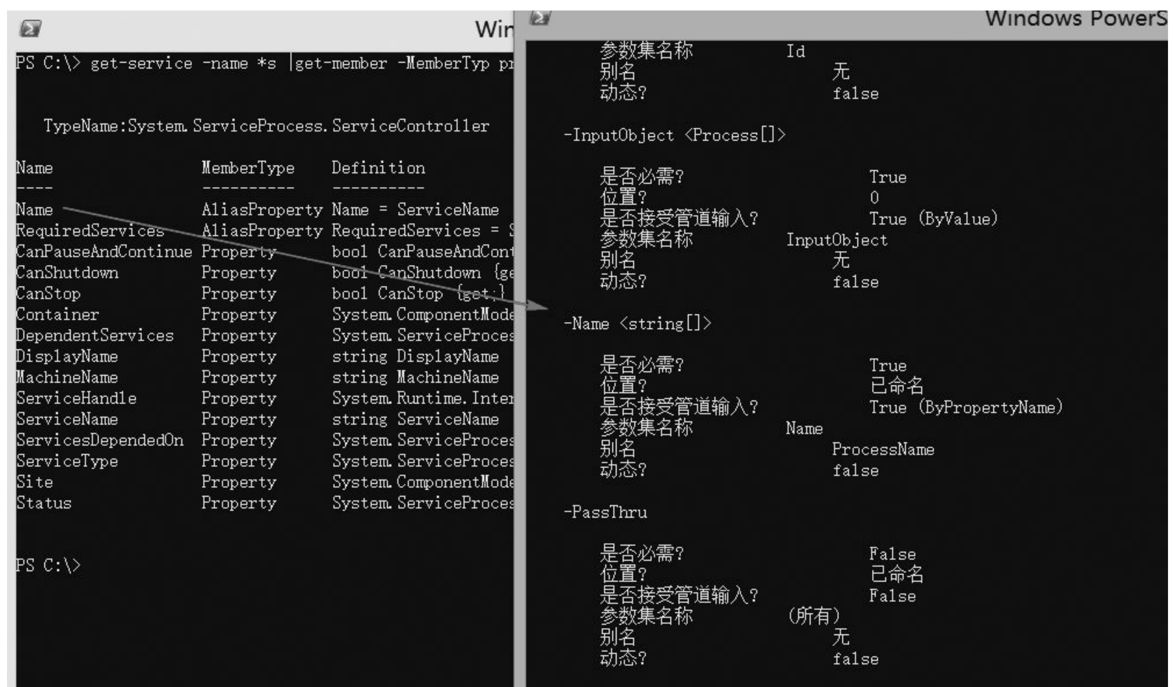
　　□□□□□□□□□A□□□□□□□□□B□□□□□ByPropertyName□ByValue□□□□□□□□□□□□B□□□□□□□□□□□□□□□□□□A□□□□□□□Get-Member□□□□□□□B□□□□□9.5□□□□□□□□A□□□□□□□□□□□□□□□□B□□□□□



[illegible]9.5 [illegible]

[illegible]Shell[illegible]“Name”[illegible]“-Name”[illegible]Shell[illegible]

[illegible]-Name[illegible]ByPropertyName[illegible]9.6[illegible]



[illegible]9.6 [illegible]Stop-Process[illegible]-Name[illegible]ByPropertyName[illegible]

□□□□□□□-Name□□□□□□□□ByPropertyName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ByValue□□□□□□□□□□□□□ByPropertyName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ByPropertyName□□□□□□□□□□□□□□□□□□Name□□□-Name□□□□□□□9.7□□□

□□9.7□□□□□□□□□□□□□□□□□□□□Service□□□□□□□□□□ShellHWDetection□SessionEnv□□□□□□□□□□□□□□□□□svchost.exe□□□□□□□□Stop-Process□□□□□□□□□□□□□□□□□□Name□□□□□□□□□□-Name□□□□□Name□□□□□□□□□□□□□-Name□□□□□□□□□□□□□□□□□□□□

```
PS C:\> get-service -name s* |stop-process -whatif
stop-process : 找不到名为“SamSs”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (SamSs:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand

stop-process : 找不到名为“SCardSvr”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (SCardSvr:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand

stop-process : 找不到名为“ScDeviceEnum”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (ScDeviceEnum:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand

stop-process : 找不到名为“Schedule”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Schedule:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand

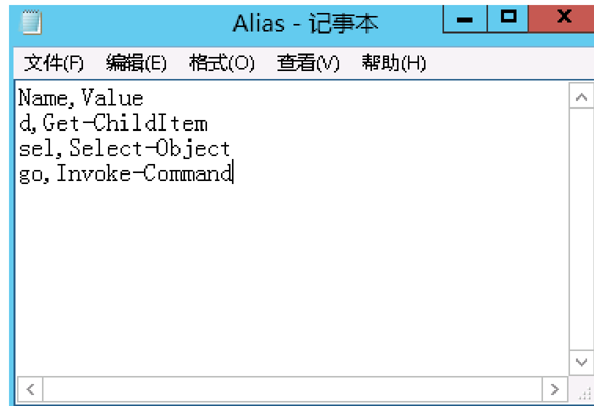
stop-process : 找不到名为“SCPolicySvc”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (SCPolicySvc:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand

stop-process : 找不到名为“seclogon”的进程。请验证该进程名称，然后再次调用 cmdlet。
所在位置 行:1 字符: 23
+ get-service -name s* |stop-process -whatif
+                       ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (seclogon:String) [Stop-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.StopProcessCommand
```

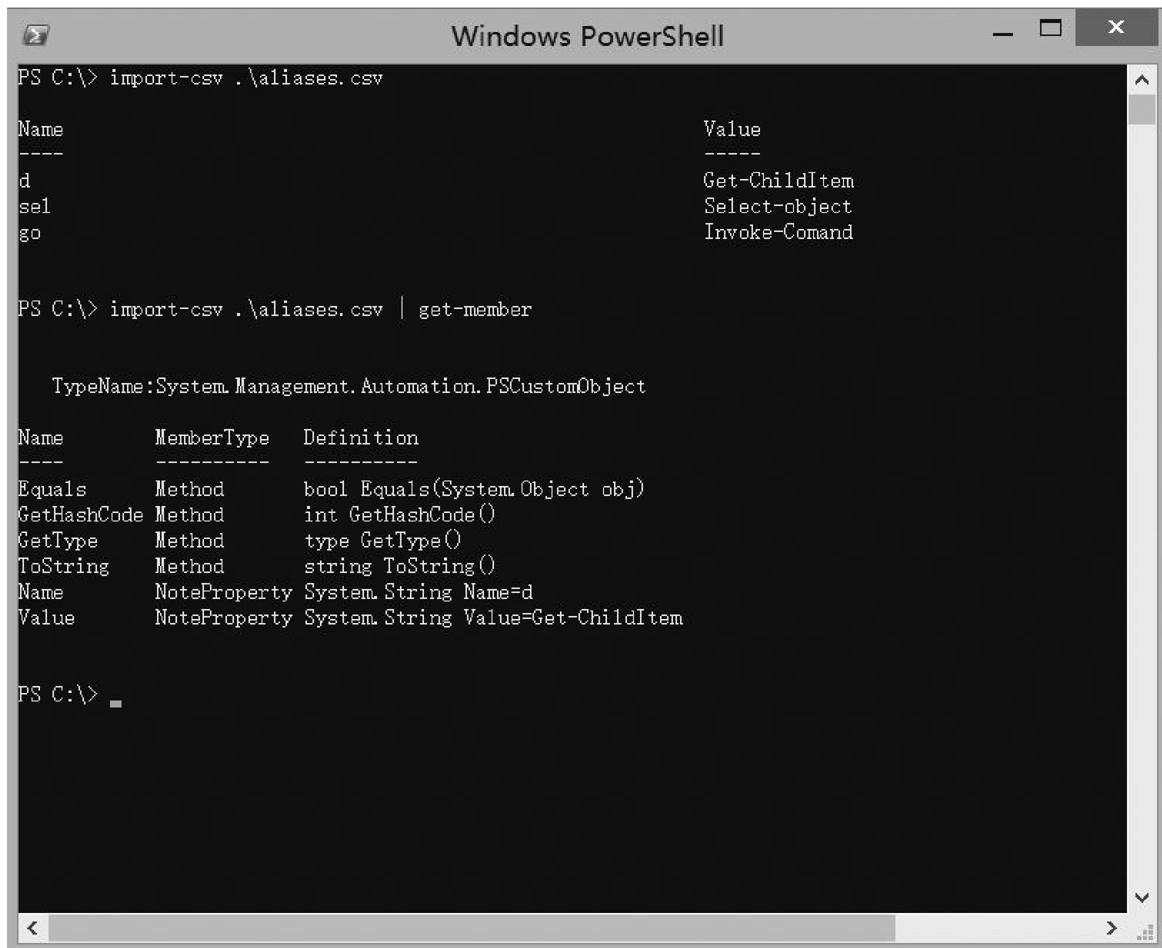
□9.7 □□□Get-Service□□□□□□□□□□□□Stop-Process

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CSV□□□□□9.8□□□

□□□□□□□Alias.CSV□□□□□Shell□□□□□□□□□□□□□□9.9□□□□□□□□□□□Import-CSV□□□□□□□□□□□□Get-Member□□□□□□□□□□□□□□□

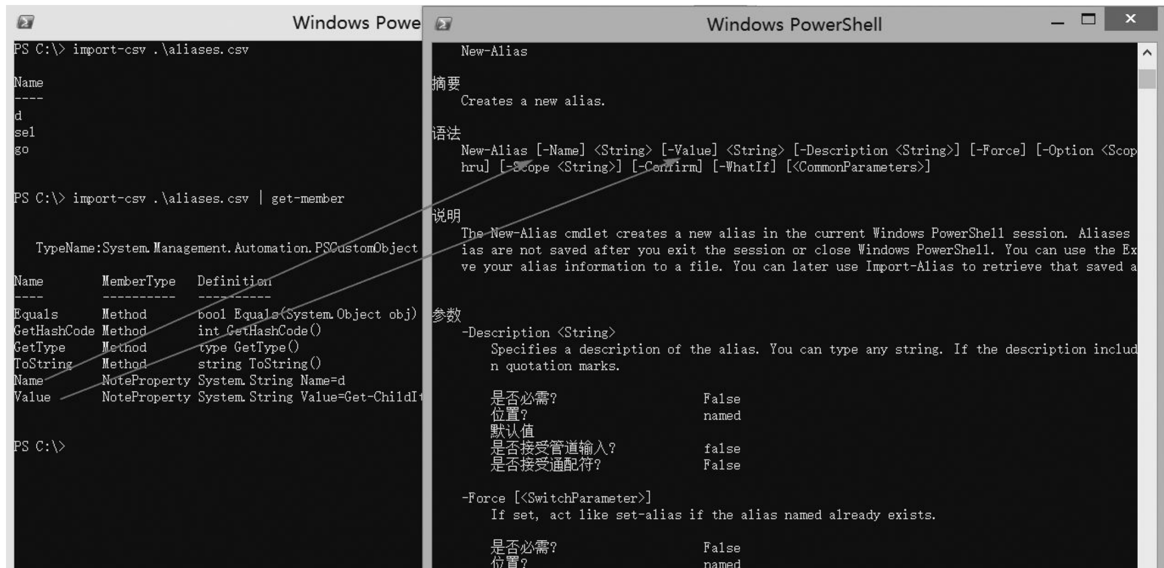


□9.8 □Windows□□□□□□CSV□□



□9.9 □□CSV□□□□□□□□□□

□□□□□□□□□CSV□□□□□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□□□New-Alias□□□□□□□□9.10□□□



□9.10 □□□□□□□□□□

Name□Value□□□□□□□□New-Alias□□□□□□□□□□□□□□□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□New-Alias□-Name□-Value□□□□□□□□□□ByPropertyName□□□□□□□□□□9.11□□□

□□

```
PS C:\>Import-CSV .\aliases.csv | New-Alias
```

□□□□□□□□□□□□□□□□□□d□sel□go□□□□□Get-ChildItem□Select-Object□Invoke-Command□□□



□9.11 □□□□ByPropertyName□□□□□□

9.5 □□□□□□□□

□□□□□□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□New-ADUser□□□□□□□□□□□□□□□□□□□Windows Server 2008 R2□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Remote Server Administration Tools□RSAT□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

New-ADUser□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

- -Name□□□□□□□□
- -samAccountName□□□□□□□□□□□□□□□□□□□□□□□□AD□□□□
- -Department
- -City
- -Title

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ByPropertyName□□□□□□□□□

[illegible]CSV[illegible]HR[illegible]HR[illegible]9.12[illegible]



[illegible]9.12 [illegible]HR[illegible]CSV[illegible]

[illegible]9.12[illegible]PowerShell[illegible]CSV[illegible]dept[illegible]New-ADUser[illegible]-Department[illegible]Login[illegible]samAccountName[illegible]Name[illegible]

```
PS C:\>Import-CSV .\NewUsers.CSV | New-AdUser
```

[illegible]CSV[illegible]New-ADUser[illegible]PowerShell[illegible]Shell[illegible]

```
PS C:\> Import-CSV .\NewUsers.CSV |
>> Select-Object -Property *,
>> @{name='samAccountName';expression={$_.login}},
>> @{label='Name';expression={$_.login}},
>> @{n='Department';e={$_.Dept}}
>>
```

```
Login            : DonJ
Dept             : IT
City             : Las Vegas
Title            : CTO
SamAccountName  : DonJ
Name             : DonJ
Department      : IT

Login            : GregS
Dept             : Custodial
City             : Denver
Title            : Janitor
samAccountName  : GregS
Name             : GregS
Department      : Custodial

Login            : JeffH
Dept            : IT
City            : Syracuse
Title           : NetWork Engineer
SamAccountName : JeffH
Name            : JeffH
Department     : IT
```

[illegible]

- [illegible]Select-Object[illegible]-Property[illegible]*[illegible]*[illegible]“[illegible]”[illegible]*[illegible]
- [illegible]@{[illegible]}[illegible]-[illegible]Key-Value[illegible]Select-Object[illegible]
- Select-Object[illegible]Name[illegible]N[illegible]Label[illegible]L[illegible]samAccountName[illegible]Name[illegible]Department[illegible]New-ADUser[illegible]
- Select-Object[illegible]expression[illegible]E[illegible]{}[illegible]$_[illegible]CSV[illegible]$_[illegible]CSV[illegible]

[illegible] [illegible]9.12[illegible]CSV[illegible]

[illegible]CSV[illegible]Import-CSV[illegible]New-ADUser[illegible]AD[illegible]

```
PS C:\> Import-CSV .\NewUsers.CSV |
>> Select-Object -Property *,
>> @{name='samAccountName';expression={$_.login}},
>> @{label='Name';expression={$_.login}},
>> @{n='Department';e={$_.Dept}} |
>> New-ADUser
>>
```

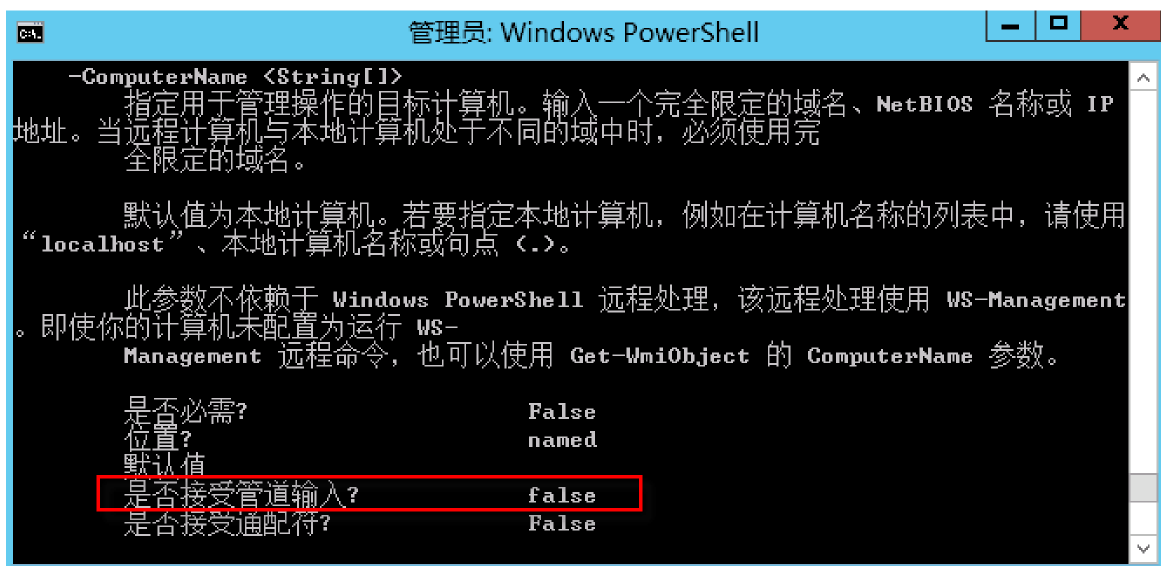
[illegible]PowerShell[illegible]PowerShell[illegible]Help Select –Example[illegible]

9.6 [illegible]

[illegible]Get-WMIObject[illegible]9.13[illegible]

[illegible]

```
PS C:\>Get-Content .\computers.txt |Get-WMIObject -Class win32_bios
```



[illegible]9.13 [illegible]Get-WMIObject[illegible]

Get-Content[illegible]String[illegible]Get-WMIObject[illegible]-ComputerName[illegible]

```
PS C:\> Get-WMIObject -Class Win32_BIOS -ComputerName
(Get-Content .\computers.txt)
```

[illegible]“[illegible]”[illegible]PowerShell[illegible]String[illegible]Get-WMIObject[illegible]-ComputerName[illegible]String[illegible]

[illegible] [illegible]IP[illegible]computers.txt[illegible]

[illegible]——[illegible]

9.7 [illegible]

[illegible]Get-Content[illegible]Cmdlet[illegible]

```
Get-Service -computerName (Get-Content names.txt)
```

[illegible]ActiveDirectory[illegible]Windows Server 2008 R2[illegible]RSAT[illegible]Domain Controller[illegible]

```
PS C:\>Get-ADComputer -Filter * -SearchBase "ou=domain controllers,
➥dc=company,dc=pri"
```

[illegible]Get-Service[illegible]

```
PS C:\>Get-Service -computerName (Get-ADComputer -filter *
➥-searchBase "ou=domain controllers,dc=company,dc=pri")
```

[illegible]

[illegible]Get-ADComputer[illegible]

[illegible]ActiveDirectory[illegible]Windows 2008 Server R2[illegible]RSAT[illegible]

[illegible]

[illegible]-Filter *[illegible]-SearchBase[illegible]Company.com[illegible]

```
Get-ADComputer -Filter * -SearchBase "ou=domain
➥controllers,dc=company,dc=pri"
```

[illegible]Name[illegible]

[illegible]

[illegible]Get-Service[illegible] [illegible]-Computer[illegible]String[illegible]

[illegible]

```
Get-ADComputer -Filter * -SearchBase "ou=domain controllers,
➥dc=company,  dc=pri" | gm
```

[illegible]Get-Member[illegible]Get-ADComputer[illegible]ADComputer[illegible]String[illegible]-ComputerName[illegible] [illegible]ADComputer[illegible]-Name[illegible]ADComputer[illegible]-Name[illegible]-ComputerName[illegible]

> **[illegible]** [illegible]PowerShell[illegible]Get-Member[illegible]Get-ADComputer[illegible]ADComputer[illegible]-ComputerName[illegible]String[illegible]ADComputer[illegible]

[illegible]Select-Object[illegible]-ExpandProperty[illegible]Select-Object[illegible]

```
Get-ADComputer -Filter * -SearchBase "ou=domain controllers,
➡dc=company,  dc=pri" | Select-Object -expand name
```

[illegible]Get-Service[illegible]-ComputerName[illegible]-ComputerName[illegible]Cmdlet[illegible]

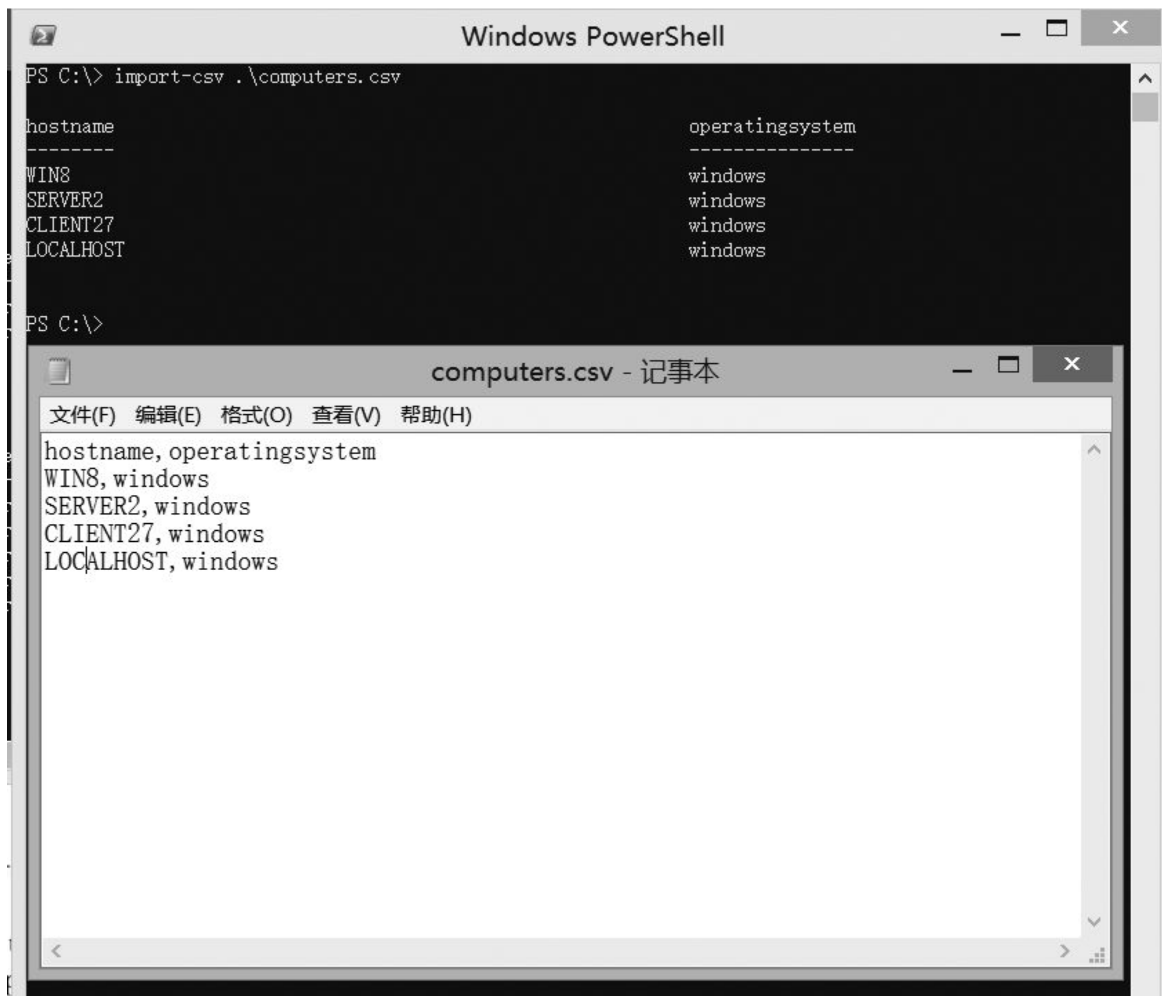
```
Get-Service -ComputerName (Get-ADComputer -Filter *
➡-SearchBase "ou=domain controllers,dc=company,dc=pri"|
➡Select-Object -Expand name)
```

> **[illegible]** [illegible]Select-Object –Property Name[illegible]Name[illegible]-ComputerName[illegible]-Name[illegible]String[illegible]-ExpandName[illegible]Name[illegible]String[illegible]

[illegible]PowerShell[illegible]

[illegible]Get-ADComputer[illegible]

[illegible]CSV[illegible]9.14[illegible]CSV[illegible]HostName[illegible]LocalHost[illegible]3[illegible]4[illegible]



□9.14 □□□□□□Import-CSV□□□CSV□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-Process□□□□□□□□□□□□□□-ComputerName□□□□□□□ByPropertyName□□□□□□□□□□□□□□□□String□□-ComputerName□□□□String□□□□□□

```
    Get-Process -InputObject <Process[]> [-ComputerName <string[]>] [-Module] [-FileVersionInfo]  [<

参数
    -ComputerName <string[]>

        是否必需?                    False
        位置?                        已命名
        是否接受管道输入?            True (ByPropertyName)
        参数集名称          InputObject, Name, Id
        别名                     Cn
        动态?                    false

    -FileVersionInfo

        是否必需?                    False
        位置?                        已命名
        是否接受管道输入?            False
        参数集名称          Name, InputObject, Id
        别名                     FV, FVI
        动态?                    false

    -Id <int[]>

        是否必需?                    True
        位置?                        已命名
        是否接受管道输入?            True (ByPropertyName)
        参数集名称          IdWithUserName, Id
        别名                     PID
        动态?                    false

    -IncludeUserName
-- More  --
```

□9.15 □□-ComputerName□□□□□□□□□

□□□□□□□□□□□□□□□□□□Get-Member□□□□A□□□□□9.16□□□□□□

```
PS C:\> import-csv .\computers.csv | get-member


   TypeName:System.Management.Automation.PSCustomObject

Name            MemberType   Definition
----            ----------   ----------
Equals          Method       bool Equals(System.Object obj)
GetHashCode     Method       int GetHashCode()
GetType         Method       type GetType()
ToString        Method       string ToString()
hostname        NoteProperty System.String hostname=WIN8
operatingsystem NoteProperty System.String operatingsystem=windows


PS C:\>
```

□9.16 Import-CSV□□□□PSCustomObject□□□□

Import-CSV□PSCustomObject□□□□□□String□□□□□□□□□□□

```
PS C:\> Get-Process -ComputerName (Import-CSV .\Computers.CSV)
```

□□□□CSV□□□□□HostName□□□□□□□□□□□□9.17□□□

```
PS C:\> import-csv .\computers.csv | select -property hostname | get-member


   TypeName:Selected.System.Management.Automation.PSCustomObject

Name        MemberType   Definition
----        ----------   ----------
Equals      Method       bool Equals(System.Object obj)
GetHashCode Method       int GetHashCode()
GetType     Method       type GetType()
ToString    Method       string ToString()
hostname    NoteProperty System.String hostname=WIN8


PS C:\>
```

□9.17 □□□□□□□□□□PSCustomObject□□

□□□□□PSCustomObject□□□□□□□□□□□□□□□□□□□□□□
Select-Object□-Property□□□□□□□□□□□□□□□□□□□□□□

□□-ComputerName□□□□□□□□□PSCustomObject□□□□□□□□□□□□
□□□□□□□□□

```
PS C:\> Get-Process -ComputerName (Import-CSV .\Computers.CSV |
Select -Property HostName)
```

□□□□□-ExpandProperty□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□9.18□□□

□□HostName□□□□□□□□□□□-ExpandProperty□□□□□□□□□□□□□□□□
□□□String□□□□□□□-ComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\>Get-Process -ComputerName (Import-CSV .\Computers.CSV |
Select -Expand HostName)
```

□□□
□□□□□□□□□□Select-Property□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□Select -ExpandProperty□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□

```
Windows PowerShell
PS C:\> import-csv .\computers.csv | select -expand hostname | get-member


   TypeName:System.String

Name             MemberType           Definition
----             ----------           ----------
Clone            Method               System.Object Clone(), System.Object ICloneable.Clone()
CompareTo        Method               int CompareTo(System.Object value), int CompareTo(string strB
Contains         Method               bool Contains(string value)
CopyTo           Method               void CopyTo(int sourceIndex, char[] destination, int destinat
EndsWith         Method               bool EndsWith(string value), bool EndsWith(string value, Syst
Equals           Method               bool Equals(System.Object obj), bool Equals(string value), bo
GetEnumerator    Method               System.CharEnumerator GetEnumerator(), System.Collections.IEn
GetHashCode      Method               int GetHashCode()
GetType          Method               type GetType()
GetTypeCode      Method               System.TypeCode GetTypeCode(), System.TypeCode IConvertible.G
IndexOf          Method               int IndexOf(char value), int IndexOf(char value, int startInd
IndexOfAny       Method               int IndexOfAny(char[] anyOf), int IndexOfAny(char[] anyOf, in
Insert           Method               string Insert(int startIndex, string value)
IsNormalized     Method               bool IsNormalized(), bool IsNormalized(System.Text.Normalizat
LastIndexOf      Method               int LastIndexOf(char value), int LastIndexOf(char value, int
LastIndexOfAny   Method               int LastIndexOfAny(char[] anyOf), int LastIndexOfAny(char[] a
Normalize        Method               string Normalize(), string Normalize(System.Text.Normalizatio
PadLeft          Method               string PadLeft(int totalWidth), string PadLeft(int totalWidth
PadRight         Method               string PadRight(int totalWidth), string PadRight(int totalWid
Remove           Method               string Remove(int startIndex, int count), string Remove(int s
Replace          Method               string Replace(char oldChar, char newChar), string Replace(st
Split            Method               string[] Split(Params char[] separator), string[] Split(char[
StartsWith       Method               bool StartsWith(string value), bool StartsWith(string value,
Substring        Method               string Substring(int startIndex), string Substring(int startI
ToBoolean        Method               bool IConvertible.ToBoolean(System.IFormatProvider provider)
ToByte           Method               byte IConvertible.ToByte(System.IFormatProvider provider)
```

[illegible]9.18 [illegible]String[illegible]

9.8 [illegible]

[illegible] [illegible]3.0[illegible]PowerShell[illegible]

[illegible]

[illegible]Get-ADComputer[illegible] Windows Server 2008 R2[illegible]

- Get-ADComputer[illegible]-Filter[illegible]Get-ADComputer-Filter*[illegible]

- [illegible]Name[illegible]
- [illegible]ADComputer[illegible]Get-ADComputer [illegible]ADComputer[illegible]

[illegible]

> **[illegible]** [illegible]Get-ADComputer[illegible]

1[illegible]Hotfix[illegible]

```
Get-HotFix -ComputerName (Get-ADComputer -Filter * |
Select-Object -Expand Name)
```

2[illegible]HotFix[illegible]

```
Get-ADComputer -Filter * |
Get-HotFix
```

3[illegible]HotFix[illegible]

```
Get-ADComputer -Filter * |
Select-Object @{l='ComputerName';e={$_.Name}} |
Get-HotFix
```

4[illegible]

5[illegible]

6[illegible]Cmdlet[illegible]

```
Get-ADComputer -Filter * |
   Select-Object @{l='ComputerName';e={$_.Name}} |
Get-WMIObject -Class Win32_BIOS
```

9.9 [illegible]

[illegible] MoreLunches.Com[illegible]“[illegible]”[illegible]Get-Service | Stop-Service[illegible]

[illegible]10[illegible] [illegible]

[illegible]PowerShell Cmdlets[illegible]PowerShell[illegible]“Gm”[illegible]“Select-Object”[illegible]PowerShell[illegible]

10.1 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]

10.2 [illegible]

[illegible]“Get-Process”[illegible]PowerShell[illegible]“.format.pslxml”[illegible]“DotNetTypes.format.pslxml”[illegible]

[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]“DotNetType.format.pslxml”[illegible]PowerShell[illegible]

```
PS C:\>cd $pshome
PS C:\>notepad dotnettypes.format.ps1xml
```

[illegible]“Get-Process”[illegible]

```
PS C:\>get-process | gm
```

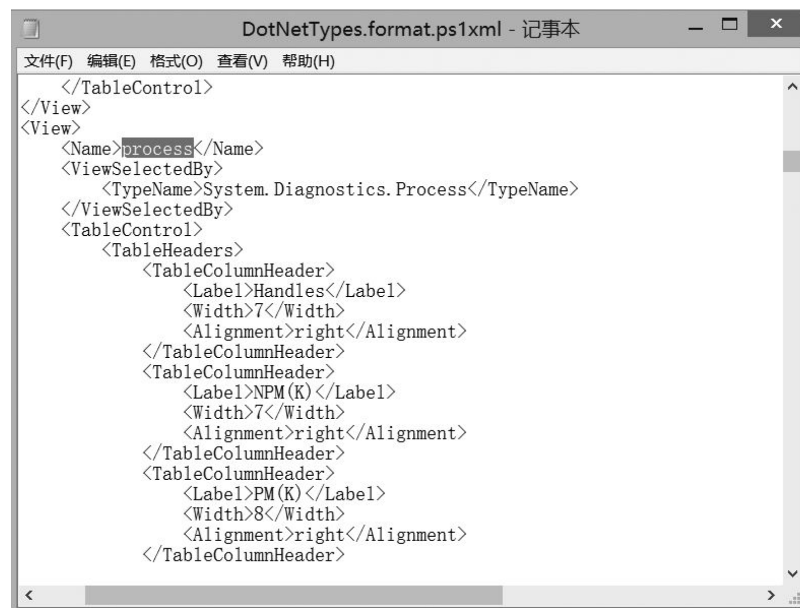
□□□□□□□□□□□□

□1□□□□□□□□□□□System.Diagnostics.Process□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□2□□□□□□□□□□□□Ctrl+F□□□□□□□□□□□

□3□□□□□□□□□□□□□□□□“□□□□□□”□

□4□□□□□□□□□□□□□□□“ProcessModule”□□□□□□□□□□□□□□□□□□□□□□□□□□□“System.Diagnostics.Process”□□□□□10.1□□□




```
    </TableControl>
</View>
<View>
    <Name>process</Name>
    <ViewSelectedBy>
        <TypeName>System.Diagnostics.Process</TypeName>
    </ViewSelectedBy>
    <TableControl>
        <TableHeaders>
            <TableColumnHeader>
                <Label>Handles</Label>
                <Width>7</Width>
                <Alignment>right</Alignment>
            </TableColumnHeader>
            <TableColumnHeader>
                <Label>NPM(K)</Label>
                <Width>7</Width>
                <Alignment>right</Alignment>
            </TableColumnHeader>
            <TableColumnHeader>
                <Label>PM(K)</Label>
                <Width>8</Width>
                <Alignment>right</Alignment>
            </TableColumnHeader>
```

□10.1 □Windows□□□□□□□□□□

□□PowerShell□

□□□“Get-Process”□□Shell□□□□□□□□□□□

□1□Cmdlet□□□□“System.Diagnostics.Process”□□□□□□□□□

□2□□□□□□□□□□□□“Out-Default”□□□□Cmdlet□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□

□3□“Out-default”□□□□□□“Out-Host”□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□host□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□4□□□□“Out-Cmdlets”□□□□□□□□□□□□□□□□□□□□□□□□□□“Out-Host”□□□□□□□□□□□□□□□□□□□□□

□5□□□“Out-Host”□

□6□□□“Out-Host”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□“Out-Cmdlet”□□□□□□□□□“Get-Process | Out-File procs.txt”□“Out-File”□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Out-File”□“Out-File”□□

□□□12□□□PowerShell□□□“DotNetType.format.ps1xml”□□□□□□□□PowerShell□□□□□□□“.format.ps1xml”□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“System.Diagnostics.Process”□□□□□

□□□□□□□□□□□□□□□□□□□□

```
Get-WmiObject Win32_OperatingSystem | Gm
```

□□□□□□□□□□□□□“Win32_OperatingSystem”□□□□□□□□□□□□□“.format.ps1xml”□□□□□□□□□□□□□□□□□□□□□ □□□□

□□□“default display property set”□□□□□□□□□□□□□“Types.ps1xml”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Win32_OperatingSystem”□□□□□□□□□□□□□□□□□□□□□“DefaultDisplayPropertySet”□□□10.2□□□□□□□□□6□□□□



□10.2 □□□□□□□DefaultDisplayPropertySet

□□□□PowerShell□□□□□

```
Get-WmiObject Win32_OperatingSystem
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□“Types.ps1xml”□□□□□□□□□□□□□“default display property set”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□——□□□□□□□□□□□□□□□4□□□□□□□□□□□□□□□□□5□□□□□□□□□□□□□□“Win32_OperatingSystem”□□□□□□□□□□□□□□□6□□□□□□□□□□□□□□□□□4□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□“Out-Cmdlets”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

10.3 □□□□□

□PowerShell□□4□□□□Cmdlets□□□□□□□□□□3□□□4□□□□□□“□□□□”□□□□□□□□“Format-Table”□□□□“Ft”□

□□□□“Format-Table”□□□□□□□□□□□□□□□□□□□□□□□□□□

- -autoSize——□□□□□PowerShell□□□“-autoSize”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

Shell[illegible]
[illegible]“-autoSize”[illegible]

```
Get-WmiObject Win32_BIOS | Format-Table –autoSize
```

- -property——[illegible]Shell[illegible]“CPU”[illegible]“cpu”[illegible]“*”[illegible]“c*”[illegible]c[illegible]Shell[illegible]10.3[illegible]

```
Get-Process | Format-Table -property *
Get-Process | Format-Table -property ID,Name,Responding -autoSize
Get-Process | Format-Table * -autoSize
```

- -groupBy——[illegible]

```
Get-Service | Sort-Object Status | Format-Table -groupBy Status
```

- -wrap——[illegible]Shell[illegible]…[illegible]Shell[illegible]

```
Get-Service | Format-Table Name,Status,DisplayName -autoSize –wrap
```

```
PS C:\> ps | ft -auto

Handles NPM(K)  PM(K)  WS(K) VM(M)   CPU(s)    Id ProcessName
------- ------  -----  ----- -----   ------    -- -----------
    161     20   3344   4548   100           2268 AppleMobileDeviceService
     85      6   1396   1384   114           5552 appverif
     85      6   1396   1388   114           5568 appverif
     85      6   1392   1388   114           5584 appverif
     84      9   9072   2708    65           5608 appverif
     72      6    972   2020    17           1844 AsLdrSrv
    155     15   3356   9744    99     0.06  7532 AsusTPCenter
     46      6   1156   4448    50     0.02  6676 AsusTPHelper
    136     11   1976   8604    82     0.08  9008 AsusTPLoader
     65      5    804    880    42           5800 AtBroker
     65      5    792    880    42           5816 AtBroker
     65      5    808    884    42           5840 AtBroker
     65      5    808    892    42           5872 AtBroker
    100     13   2336  10364   114     0.14  3640 ATKOSD2
    140      9   6124   9080    39     0.36  7148 audiodg
    122     10  15628  14964    98           3652 bootim
    122     10  15844  15076    98           5216 bootim
    122     10  15632  15124    98           5576 bootim
    122     10  15716  15100    98           5748 bootim
    116     12   4568   4600    78           5208 calc
    116     12   4584   4632    78           5624 calc
    116     12   4580   4612    78           5704 calc
    116     12   4584   4604    78           5808 calc
     70      8   1424   5944    74     0.03 10296 caller64
     90      7   1248   1508    30           5144 CameraSettingsUIHost
     92      7   1260   1508    30           5212 CameraSettingsUIHost
```

□10.3 □□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

10.4 □□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Format-List”□□□□□□□□□□□□□□□□□□Fl□

□□Cmdlet□□□□□□□□□□□□“Format-Table”□□□“-property”□□□□□Fl□□□□□□□□□□□□□□□□□Gm□□□□Fl□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
Get-Service | Fl *
```

□10.4□□□□□□□□□□□□□□□Fl□□□□□□□□□□□□□□

```
ServiceName         : NcaSvc
ServicesDependedOn  : {NSI, dnscache, iphlpsvc, BFE}
ServiceHandle       :
Status              : Stopped
ServiceType         : Win32ShareProcess
Site                :
Container           :

Name                : NcbService
RequiredServices    : {RpcSS, tcpip}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : True
DisplayName         : Network Connection Broker
DependentServices   : {}
MachineName         : .
ServiceName         : NcbService
ServicesDependedOn  : {RpcSS, tcpip}
ServiceHandle       :
Status              : Running
ServiceType         : Win32ShareProcess
Site                :
Container           :

Name                : NcdAutoSetup
RequiredServices    : {netprofm}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : True
DisplayName         : Network Connected Devices Auto-Setup
```

□10.4 □□□□□□□□□□

□□□□□“Format-List”□□□□□□□□□□□□□□

10.5 □□□□□

□□□□□□□Cmdlet□“Format-Wide”□□□□Fw□□□□□□□□□□□□□□□□□□□□“-property”□□□□□□□□□□□□□□□□□□□

□□□□“Format-Wide”□□□□“Name”□□□□“Name”□□□□□□□□□□□□□□□□□□□□□□“-columns”□□□□□□□□□

```
Get-Process | Format-Wide name -col 4
```

□10.5□□□□□

```
选定 Windows PowerShell
PS C:\> get-process | format-wide name -col 4


AppleMobileDeviceService     appverif                     appverif                     appverif
appverif                     AsLdrSrv                     AsusTPCenter                 AsusTPHelper
AsusTPLoader                 AtBroker                     AtBroker                     AtBroker
AtBroker                     ATKOSD2                      audiodg                      bootim
bootim                       bootim                       bootim                       calc
calc                         calc                         calc                         caller64
CameraSettingsUIHost         CameraSettingsUIHost         CameraSettingsUIHost         CameraSettingsUIHost
CertEnrollCtrl               CertEnrollCtrl               CertEnrollCtrl               CertEnrollCtrl
certreq                      certreq                      certreq                      certreq
changepk                     charmap                      charmap                      charmap
charmap                      choice                       choice                       choice
choice                       chrome                       chrome                       chrome
chrome                       chrome                       chrome                       chrome
chrome                       cleanmgr                     cliconfg                     cliconfg
cliconfg                     cliconfg                     cmd                          cmd
cmd                          cmd                          cmd                          cmd
cmd                          cmd                          cmd                          comp
conhost                      conhost                      conhost                      conhost
conhost                      conhost                      conhost                      conhost
conhost                      conhost                      conhost                      conhost
conhost                      conhost                      conhost                      conhost
conhost                      conhost                      conhost                      conhost
CSISYN~1                     csrss                        csrss                        csrss
csrss                        csrss                        csrss                        dasHost
DBMon_ABC                    DBSer_ABC                    DhMachineSvc                 DhPluginMgr
dllhost                      DMedia                       dwm                          explorer
explorer                     FlashUtil_ActiveX            Foxit Reader                 Foxmail
Foxmail                      Foxmail                      FSCapture                    HControl
HeciServer                   hkcmd                        IAStorIcon                   ICCProxy
Idle                         iexplore                     iexplore                     iexplore
iexplore                     iexplore                     igfxpers                     igfxsrvc
IntelMeFWService             iPodService                  ipoint                       iTunesHelper
itype                        logread                      lsass                        notepad
notepad                      notepad                      NvBackend                    nvSCPAPISvr
nvtray                       nvvsvc                       nvvsvc                       nvxdsync
powershell                   PresentationFontCache        QMChExt                      QQ
QQPCNetFlow                  QQPCRealTimeSpeedup          QQPCRTP                      QQPCTray
QQProtect                    QuickGesture                 QuickGesture64               SearchFilterHost
SearchIndexer                SearchProtocolHost           services                     SettingSyncHost
```

□10.5 □□□□□□□□□□□□□

□□□□□□□□□□“Format-Wide”□□□□□□□□□□□□□□□□□□□□□□□□□□□

10.6 □□□□□□□□

□□□□□□□□□□□9.5□□“□□□□□□□□□□□□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Format-Table”□“Format-List”□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
Get-Service |
Format-Table @{n='ServiceName';e={$_.Name}},Status,DisplayName
```

□□□□□□□□□□□□□□□□□

```
Get-Process |
Format-Table Name,
@{n='VM(MB)';e={$_.VM / 1MB -as [int]}} –autosize
```

□10.6□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□

- □□□“Get-Process”□□□□□□□□□□□□□□□□□□□□□□□□“Get-Process | Fl *”□□□□□□“VM”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□“Name”□□□□□□“Format-Table”□

```
Windows PowerShell
PS C:\> Get-Process | Format-Table Name,@{n='VM(MB)';e={$_.VM / 1MB -as [int]}} -autosize

Name                     VM(MB)
----                     ------
AppleMobileDeviceService    100
appverif                    114
appverif                    114
appverif                    114
appverif                     65
AsLdrSrv                     17
AsusTPCenter                 99
AsusTPHelper                 50
AsusTPLoader                 82
AtBroker                     42
AtBroker                     42
AtBroker                     42
AtBroker                     42
ATKOSD2                     114
audiodg                      39
bootim                       98
bootim                       98
bootim                       98
bootim                       98
calc                         78
calc                         78
calc                         78
calc                         78
caller64                     74
CameraSettingsUIHost         30
CameraSettingsUIHost         30
CameraSettingsUIHost         30
CameraSettingsUIHost         30
```

□10.6 □□□□□□□□□□□□□□MB□

- □□□□□□□□□□“VM(MB)”□□□□□□□□□□□□□□□□□□□□□□□□VM□□□□□□1 MB□□PowerShell□□□□□□□□□□□□□□□“KB”“MB”“GB”“TB”□“PB”□□□□□□kilobyte□megabyte□gigabyte□terabyte□petabyte□
- □□□□□□□□□□□□□□□□□□“-as”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□[int]□□□□Shell□□

□□□□

□□□□□□□□□□□□□□

```
Get-Process |
Format-Table Name,
@{n='VM(MB)';e={$_.VM / 1MB -as [int]}} –autosize
```

□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□

[illegible]

[illegible]“[illegible]”[illegible]Ctrl+C[illegible]
[illegible]
Shell[illegible]Shell[illegible]

[illegible]“*”[illegible]“+/-”[illegible]

[illegible]“Select-Object”[illegible]N[illegible]L[illegible]
Label[illegible]E[illegible]“Format-”[illegible]
[illegible]“Format-Table”[illegible]

- FormatString[illegible]MSDN[illegible]“Formatting Types”[illegible]http://msdn.microsoft. com/en-us/library/26etazsy.aspx[illegible]
- Width[illegible]
- Alignment[illegible]

[illegible]

```
Get-Process |
Format-Table Name,
@{n='VM(MB)';e={$_.VM};formatstring='F2';align='right'} –autosize
```

[illegible]PowerShell[illegible]

10.7 [illegible]

[illegible]

[illegible]“Format-Cmdlet”[illegible]“Format-Cmdlet”[illegible] “Out-Default”[illegible]“Out-Host”[illegible]

```
Get-Service | Format-Wide
```

[illegible]“Out-Host”[illegible]

```
Get-Service | Format-Wide | Out-Host
```

[illegible]“Out-File”[illegible]“Out-Printer”[illegible]“[illegible]”[illegible]“Out-”Cmdlet[illegible]“Format-”Cmdlet[illegible]

[illegible]“Out-Printer”[illegible]“Out-File”[illegible]Cmdlets[illegible]“-width”[illegible]

10.8 [illegible]

“Out-GridView”[illegible]“Out-GridView”[illegible]“Format-”Cmdlets[illegible]“Out-GridView”[illegible]“Format-”Cmdlet[illegible]Cmdlets[illegible]

[illegible]10.7[illegible]

Windows PowerShell

PS C:\> get-process | out-gridview
PS C:\>

get-process | out-gridview

[illegible]

[illegible]

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
161	20	3344	4548	100		2,268	AppleMobileDeviceService
85	6	1396	1384	114		5,552	appverif
85	6	1396	1388	114		5,568	appverif
85	6	1392	1388	114		5,584	appverif
84	9	9072	2708	65		5,608	appverif
72	6	972	2020	17		1,844	AsLdrSrv
155	15	3356	9744	99	0.06	7,532	AsusTPCenter
46	6	1156	4448	50	0.02	6,676	AsusTPHelper
136	11	1976	8604	82	0.08	9,008	AsusTPLoader
65	5	804	880	42		5,800	AtBroker
65	5	792	880	42		5,816	AtBroker
65	5	808	884	42		5,840	AtBroker
65	5	808	892	42		5,872	AtBroker
100	13	2336	10364	114	0.14	3,640	ATKOSD2
140	9	6128	9080	39	0.44	7,148	audiodg
122	10	15628	14964	98		3,652	bootim
122	10	15844	15076	98		5,216	bootim

[illegible]10.7 “Out-GridView” Cmdlets[illegible]

10.9 [illegible]

[illegible]PowerShell[illegible]

10.9.1 [illegible]

[illegible]format right[illegible]“Format-”Cmdlet[illegible]“Out-File”[illegible]“Out-Printer”[illegible]“Format-”Cmdlets[illegible]“Out-”Cmdlet[illegible]“Format-”Cmdlet[illegible]“Out-Default”[illegible]“Out-Host”[illegible]

[illegible]

```
Get-Service | Format-Table | Gm
```

[illegible]10.8[illegible]“Gm”[illegible]“Format-Table”Cmdlet[illegible]——[illegible]“Gm”[illegible]

```
Windows PowerShell

   TypeName:Microsoft.PowerShell.Commands.Internal.Format.GroupEndData

Name                                    MemberType Definition
----                                    ---------- ----------
Equals                                  Method     bool Equals(System.Object obj)
GetHashCode                             Method     int GetHashCode()
GetType                                 Method     type GetType()
ToString                                Method     string ToString()
ClassId2e4f51ef21dd47e99d3c952918aff9cd Property   string ClassId2e4f51ef21dd47e99d3c952918aff9cd {get;}
groupingEntry                           Property   Microsoft.PowerShell.Commands.Internal.Format.GroupingEn

   TypeName:Microsoft.PowerShell.Commands.Internal.Format.FormatEndData

Name                                    MemberType Definition
----                                    ---------- ----------
Equals                                  Method     bool Equals(System.Object obj)
GetHashCode                             Method     int GetHashCode()
GetType                                 Method     type GetType()
ToString                                Method     string ToString()
ClassId2e4f51ef21dd47e99d3c952918aff9cd Property   string ClassId2e4f51ef21dd47e99d3c952918aff9cd {get;}
groupingEntry                           Property   Microsoft.PowerShell.Commands.Internal.Format.GroupingEn

PS C:\>
```

[illegible]10.8 [illegible]Cmdlets[illegible]

[illegible]

```
Get-Service | Select Name,DisplayName,Status | Format-Table |
ConvertTo-HTML | Out-File services.html
```

[illegible]IE[illegible]Services.html[illegible]“ConvertTo-HTML”[illegible]HTML[illegible]“Format-”Cmdlet[illegible]Cmdlet[illegible]“Out-File”[illegible]“Out-Printer”[illegible]

[illegible]“Out-GridView”[illegible]“Out-”Cmdlet[illegible]

```
PS C:\>Get-Process | Out-GridView
PS C:\>Get-Process | Format-Table | Out-GridView
```

[illegible]“Out-File”[illegible]“Out-Printer”[illegible]“Format-”Cmdlet[illegible]“Out-Host”[illegible]“Format-”Cmdlet[illegible]“Format-”Cmdlet[illegible]“Out-Host”[illegible]

10.9.2 [illegible]

[illegible]

[illegible]

```
Get-Process; Get-Service
```

[illegible]10.9[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]

```
Windows PowerShell
    103       9      1404       1892    21              4180 svchost
    362      18      6708      15452    91              5744 svchost
    148      10      2436       4200    37              7836 svchost
   4640       0       892        480     4                 4 System
    376      30      8260      17904   358    13.66     2224 taskhostex
    383      76      6032       6404    90              2940 TeamViewer_Service
    661      63     48676      52096   367    55.09     5972 ThunderPlatform
    109      10      1656       2804    54     0.06     5680 TXPlatform
     93      11      1968       1024    82     0.75     1820 USBChargerPlus
    633     125     40092       9808   132              3060 vmms
    161      12      2220       2852    65              2292 vmware-usbarbitrator64
     85      19      1300       3044    56               740 wininit
    164       8      1888      12376    72              3636 winlogon
    138       9      2108       6312    32              7284 WmiPrvSE
    164      12      3032       9500    43             10288 WmiPrvSE
    183      11      3108       8704    40             12228 WmiPrvSE
    220      11      1592       1860    40              1604 WUDFHost

Status      : Stopped
Name        : AeLookupSvc
DisplayName : Application Experience


Status      : Stopped
Name        : ALG
DisplayName : Application Layer Gateway Service


Status      : Stopped
Name        : AppHostSvc
DisplayName : Application Host Helper Service
```

[illegible]10.9 [illegible]PowerShell[illegible]

[illegible]

[illegible]——[illegible]“Dir | Gm”[illegible]“DirectoryInfo”[illegible]“FileInfo”[illegible]Gm[illegible]Dir[illegible]“DirectoryInfo”[illegible]“FileInfo”[illegible]“Format-Custom” Cmdlet[illegible]

“Format-Custom”[illegible]XML[illegible]

[illegible]PowerShell[illegible]

10.10 [illegible]

阅读下列问题并加以实践：

1．请找出所有处于运行状态且进程ID比其它进程大的所有Windows，并以“Responding”属性为依据对进程实施分组，并以带有进程对象属性编号降序的方式输出每个进程对象的结果。

2．请找出所有处于运行状态且进程ID比其它进程大的所有进程，并对其分页内存使用情况以MB为单位显示。

3．请使用“Get-EventLog”的最新事件日志列表功能，并将其以格式化表的形式显示，并在此基础上显示日志名称和保留天数属性，但须以可读名称显示其中的日志名和保留天数列标题，即以“LogName”和“RetDays”显示。

4．请使用表格形式来显示服务所有服务的状态，将已停止和正在运行的服务分组到自己的表中，此时需要使用“-groupBy”参数项。

10.11 格式化规则

在开始使用格式化前，请记住下列规则：格式化操作命令“Format-” Cmdlets应该是管道中的最后一个命令，一旦格式化后对象被转换为格式化规范对象后就无法再对其进行其它操作了。

[illegible]11[illegible] [illegible]

[illegible]Shell[illegible]

11.1 [illegible]

Shell[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]

[illegible]Cmdlet[illegible]Get-Service[illegible]

```
Get-Service -name e*[illegible]*s*
```

[illegible]Get-Service[illegible]Cmdlet[illegible]

[illegible]Get- Cmdlets[illegible]-filter[illegible]-filter*[illegible]

```
Get-ADComputer -filter "Name -like '*DC'"
```

[illegible]Cmdlet[illegible]

11.2 [illegible]

“[illegible]”[illegible]Cmdlets[illegible]

□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□Get-Service□□□□□□Name□□□□□□□□□□□Get-ADComputer□□□□□□computer□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□Where-Object□□□□□□Where□□□□PowerShell Cmdlet□□□

□□□□Where-Object□□□□□□□Shell□□□□□□□□□□□□□□□□□□Shell□□Get-Cmdlet□□-filter□□□□□□□□□□□□□□□Cmdlet□□□□Get-WmiObject□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□

11.3 □□□□□

□□true□false□□□□□□□□□□□□□□□□□□□□□□□□□□□

PowerShell□□

- -eq——□□□□□5 -eq 5□□□true□□□"hello" -eq "help"□□□false□□
- -ne——□□□□□□10 -ne 5□□□true□□□"help" -ne "help"□□□false□□□□□□□□□□□□□□□□□□□□□□□□□
- -ge□-le——□□□□□□□□□□□□□□10 -ge 5□□□true□□□Get-Date -le '2012-12-02'□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- -gt□-lt——□□□□□□□□10 -lt 10□□□false□□□100 -gt 10□□□true□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□-ceq□-cne□-cgt□ -clt□-cge□-cle□

□□□□□□□□□□□□□□□□□□□□-and□-or□□□□□□□□□□□□□□□□□□□□□□□□□□□

- (5 -gt 10) -and (10 -gt 100) □□false□□□□□□□□□□□□□□□false□
- (5 -gt 10) -or (10 -lt 100) □□true□□□□□□□□□□□□□□true□

□□□□□□-not□true□false□□□□□□□□□□□□□□□true□false□□□□□□□□□□□□□□□□□□□□□□□□□□false□□□□□□□□□□□□□□□□□□□□□□□$__□□□□□□□□□□

```
$_.Responding -eq $False
```

Windows PowerShell□□□$False□ $True□□□false□true□□□□□□□□□□□□□□□

```
-not $_.Responding
```

□□Responding□□□□true□false□□-not□false□□□□true□□□□□□□□□□□□□□Responding□□false□□□□□□□□□□□□□true□□□□□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□□□□□□□□□□□□”□□□□□□□□□□-not□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□

- -like□□*□□□□□□□□□□□□□"Hello" -like "*ll*"□□□true□□□□□□□-notlike□□□□□□□□□□□□□□□□□□□-clike□-cnotlike□
- -match□□□□□□□□□□□□□□□□□-notmatch□□□□□□□□□□□□□□□□□-cmatch□-cnotmatch□□□□□□□□□□□□□□□□□□□□□□□□□

Shell□□□□□□□□□□□□□□□□□□□□□□□□□□□□$_□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□5 -eq 5□□□□□□
□□□□□□

□about_comparison_operators□□□□□□□□□□□□□□□□□□□
□□□□□25□□□□□□□□□□

□□□□ □□Cmdlet□□□□11.3□□□□PowerShell□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

- = □□
- <> □□□
- <= □□□□□
- □>= □□□□□
- □> □□
- <□□

□□□□□□□□□□□□□□AND□OR□□□Cmdlet□□□□□□□LIKE
□□□□□□□□-filter□□□□□Get-WmiObject□□□□□□□□□□□□
14□□□□Cmdlet□□□□□□□□

□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

11.4 □□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
Cmdlet□-filter□□□□□□□□□□□□□□□□□□□□GET-□Cmdlet□□□
□□Shell□□□□Cmdlet□□Where-Object□□ □□□

□□□□□□□□□□□□□□□□□□□□□□

```
Get-Service | Where-Object -filter { $_.Status -eq 'Running' }
```

-filter□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
Where□

```
Get-Service | Where { $_.Status -eq 'Running' }
```

[illegible]“where status equals running”[illegible]Where-Object[illegible]$_[illegible]true[illegible]false[illegible]false[illegible]true[illegible]Where-Object[illegible]Cmdlet[illegible]Cmdlet[illegible]Out-Default[illegible]8[illegible]

[illegible]$_[illegible]10[illegible]PowerShell[illegible]10[illegible]Shell[illegible]Status[illegible]

[illegible]Gm[illegible]PowerShell[illegible]Get-Process[illegible]PM(MB)[illegible]Get-Process | Gm[illegible]PM[illegible]Gm[illegible]Format-[illegible]Cmdlet[illegible]

[illegible]

PowerShell v3[illegible]Where-Object[illegible]“[illegible]”[illegible]

```
Get-Service | Where Status -eq 'Running'
```

[illegible]{}[illegible]$_[illegible]

```
Get-WmiObject -Class Win32\_Service |
Where { $\_.State -ne 'Running' -and $_.StartMode -eq 'Auto'
}
```

[illegible]6[illegible]“[illegible]”[illegible]

　　□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-WmiObject
□-Filter□□□□□□□□□□□□□□□□□□□□□□□□□□□□Where-Object
□“□”□□□□□□□□□□

11.5 □□□□□□□□

□□□□□□□□□□□PowerShell□□□□□□□□□□□PSICLM□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□PSICLM□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□

□□
PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□1□□□□□□□□

□2□□□PowerShell□□□

□3□□□□□□□□□□□□

□4□□□□□10□□□□□10□□□□□□□□□□□□□□

□5□□□□□□□□□□□□□□

□□□□□□□□□□□□ 3 □□□□□ 4 □□□□□□□□□□□□□□□□Select-
Object□

　　□□□□□□□□□□□□□Select-Object□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□

□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□Get-
Command□Help□□□□□□□□□□□□□add□□□□□sum□□□□□□□
Measure□□□□

　　□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Help□Get-
Command□□*□□□□

[illegible]PowerShell[illegible]
[illegible]

[illegible]

```
Get-Process
```

[illegible]Shell[illegible]
[illegible]

[illegible]“[illegible]”[illegible]
[illegible]Where-Object[illegible]Cmdlet[illegible]
[illegible]Cmdlet[illegible]

[illegible]Shell[illegible]

```
Get-Process | Where-Object -filter { $_.Name -notlike
'powerShell*' }
```

[illegible]“powerShell”[illegible]“powerShell.exe”[illegible]
[illegible]

[illegible]

```
Get-Process | Where-Object -filter { $_.Name -notlike
'powerShell*' } |
Sort VM -descending
```

[illegible]

```
Get-Process | Where-Object -filter { $_.Name -notlike
'powerShell*' } |
 Sort VM -descending | Select -first 10
```

[illegible]-last 10[illegible]

```
Get-Process | Where-Object -filter { $_.Name -notlike
'powerShell*' }|
```

```
Sort VM -descending | Select -first 10 |
Measure-Object -property VM -sum
```

[illegible]Cmdlet[illegible]

[illegible]——[illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]Shell[illegible]Cmdlets[illegible]

11.6 [illegible]

[illegible]Where-Object[illegible]

11.6.1 [illegible]

[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]

[illegible]Where-Object——[illegible]——[illegible]PowerShell[illegible]13[illegible]

11.6.2 [illegible]$_

[illegible]$_[illegible]PowerShell[illegible]Cmdlet[illegible]Cmdlet[illegible]

[illegible]——[illegible]

```
Get-Service -computername (Get-Content c:\names.txt |
Where-Object -filter { $_ -notlike '*dc' }) |
Where-Object -filter { $_.Status -eq 'Running' }
```

执行过程如下所示：

（1）逐行读取文件。将Get-Service括号中的命令行视为第一条命令执行，这里只有一条命令：Get-Content命令行。

（2）Get-Content 命令行的输出（一系列String对象）Where-Object。Where-Object的过滤条件是括号中的脚本块。$_代表从Get-Content输入进来的String对象，所以只有包含“dc”字符串的计算机名称会被Where-Object输出。

（3）Where-Object的输出结果被用于括号中的命令，Where-Object的输出结果也被用于外层Cmdlet的输入，所以名称包含“dc”的计算机名称才会被传给Get-Service的-computername参数中。

（4）最后，所有Get-Service输出的结果（ServiceController对象）被送到Where-Object中。这个Where-Object根据内部的过滤条件（$_）用于检查对象的状态属性，只输出处于启动状态的服务。

有时，您可能会觉得需要一些脑力来理解这个过程。如果是的话，请记住PowerShell是一种菜单式的方式——一旦理解了这个思路，就可以按照自己的需求来组合不同的组件。

11.7 动手实验

注　意	对于本次动手实验，您需要运行的计算机有PowerShell v3或更新版本的PowerShell的计算机。

记住，在这一章里Where-Object不是唯一的过滤方式，甚至都不应该是您首先考虑的过滤方式。我们精简了本章内容以便您可以有更多的时间用于动手实验。请记住，过滤左移原则。

1．使用NetAdapter模块（可以在安装了该模块的较新版本Windows中获得）中的Get-NetAdapter命令，显示非虚拟网络适配器（即适配器的虚拟属性Virtual为假，即false，在PowerShell中的表示为$False）。

2．使用DnsClient模块（可以在安装了该模块的较新版本Windows中获得）中的Get-DnsClientCache命令，显示本地缓存中的A和AAAA记录。提示：如果缓存为空，可以先访问几个Web页面以便在缓存中添加数据。

3[illegible]

4[illegible]Get-Service[illegible]

5[illegible]“installed by”[illegible]

6[illegible]“Conhost”[illegible]“Svchost”[illegible]“[illegible]”[illegible]

11.8 [illegible]

[illegible]Get-Hotfix[illegible]Get-EventLog[illegible]Get-Process[illegible]Get-Service[illegible]Get-Command[illegible]Get-Command[illegible]Cmdlet[illegible]Test-Connection[illegible]ping[illegible]Where-Object[illegible]

[illegible]12[illegible] [illegible]

[illegible]

12.1 [illegible]

[illegible]Windows 8[illegible]Windows Server 2012[illegible]PowerShell v3[illegible]Windows[illegible]CloudShare.com[illegible]PowerShell v3[illegible]Windows[illegible]Windows[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]3[illegible]“Accounting”[illegible]

12.2 [illegible]

[illegible]

[illegible]*print*[illegible]*printer*[illegible]

```
PS C:\> help *print*

Name            Category  Module
----            --------  ------
Add-Printer        Function   printmanagement
Add-PrinterDriver     Function  printmanagement
Add-PrinterPort      Function   printmanagement
Get-PrintConfiguration   Function   printmanagement
Get-Printer        Function   printmanagement
Get-PrinterDriver     Function   printmanagement
Get-PrinterPort      Function   printmanagement
Get-PrinterProperty     Function   printmanagement
Get-PrintJob        Function   printmanagement
```

```
Remove-Printer       Function   printmanagement
Remove-PrinterDriver    Function   printmanagement
Remove-PrinterPort     Function   printmanagement
Remove-PrintJob      Function   printmanagement
Rename-Printer       Function   printmanagement
Restart-PrintJob      Function   printmanagement
Resume-PrintJob      Function   printmanagement
Set-PrintConfiguration   Function   printmanagement
Set-Printer        Function   printmanagement
Set-PrinterProperty     Function   printmanagement
Suspend-PrintJob      Function   printmanagement
Out-Printer        Cmdlet   Microsoft.PowerShell.U
```

□□□

□□□□□□□□□□□□□□□Get-PrintJob□Remove-PrintJob□□□□□ Remove-PrintJob□□□□□□□□□□□□□□□□□□□-InputObject□□□□□□□□□□□□□□□□□□□□□□□□□□Remove-PrintJob□□□□

```
-InputObject <CimInstance#MSFT_PrintJob>

    Required?         true
    Position?         0
    Accept pipeline input?   true (ByValue)
    Parameter set name     jobObject
    Aliases         None
    Dynamic?         False
```

□□□□□□□□□□“Get-PrintJob –printer "Accounting" | Remove-PrintJob” □□

```
PS C:\> help *task*

Name               Category  Module
----               --------  ------
Disable-NetAdapterEncapsulated...  Function  NetAdapter
Enable-NetAdapterEncapsulatedP...  Function  NetAdapter
Get-NetAdapterEncapsulatedPack...  Function  NetAdapter
Set-NetAdapterEncapsulatedPack...  Function   NetAdapter
Get-CertificateNotificationTask   Cmdlet   PKI
New-CertificateNotificationTask   Cmdlet   PKI
Remove-CertificateNotification...  Cmdlet   PKI
Get-ClusteredScheduledTask     Function  ScheduledTasks
Get-ScheduledTask        Function  ScheduledTasks
Get-ScheduledTaskInfo        Function  ScheduledTasks
```

```
New-ScheduledTask           Function  ScheduledTasks
New-ScheduledTaskAction       Function  ScheduledTasks
New-ScheduledTaskPrincipal     Function  ScheduledTasks
New-ScheduledTaskSettingsSet     Function  ScheduledTasks
New-ScheduledTaskTrigger      Function  ScheduledTasks
```

[illegible]——[illegible]ScheduledTasks[illegible]

```
PS C:\> get-command -module scheduledtasks

Capability    Name
----------    ----
CIM       Get-ClusteredScheduledTask
CIM       Get-ScheduledTask
CIM       Get-ScheduledTaskInfo
CIM       New-ScheduledTask
CIM       New-ScheduledTaskAction
CIM       New-ScheduledTaskPrincipal
CIM       New-ScheduledTaskSettingsSet
Cmdlet, Script  New-ScheduledTaskTrigger
CIM       Register-ClusteredScheduledTask
CIM       Register-ScheduledTask
CIM       Set-ClusteredScheduledTask
CIM       Set-ScheduledTask
CIM       Start-ScheduledTask
CIM       Stop-ScheduledTask
CIM       Unregister-ClusteredScheduledTask
CIM       Unregister-ScheduledTask
```

[illegible]

12.3 [illegible]

[illegible]New-ScheduledTask[illegible]

```
PS C:\> help new-scheduledtask -full

NAME
     New-ScheduledTask

SYNTAX
     New-ScheduledTask [[-Action] <CimInstance#MSFT_TaskAction[]>]
     [[-Trigger] <CimInstance#MSFT_TaskTrigger[]>] [[-Settings]
     <CimInstance#MSFT_TaskSettings>] [[-Principal]
     <CimInstance#MSFT_TaskPrincipal>] [[-Description] <string>]
```

```
     [-CimSession <CimSession[]>] [-ThrottleLimit <int>] [-AsJob]
     [<CommonParameters>]
```

[illegible]-Trigger[illegible]-Action[illegible]TaskTrigger[illegible]TaskAction[illegible]

[illegible]ScheduledTask[illegible]New-ScheduledTaskTrigger[illegible]New-ScheduledTaskAction[illegible]

```
PS C:\> help New-ScheduledTaskTrigger

NAME
     New-ScheduledTaskTrigger
SYNOPSIS

SYNTAX
     New-ScheduledTaskTrigger [-RandomDelay <TimeSpan>] [-At]
<DateTime>
     -Once [<CommonParameters>]

     New-ScheduledTaskTrigger [-DaysInterval <Int32>] [-RandomDelay
     <TimeSpan>] [-At] <DateTime> -Daily [<CommonParameters>]

     New-ScheduledTaskTrigger [-WeeksInterval <Int32>] [-RandomDelay
     <TimeSpan>] [-At] <DateTime> -DaysOfWeek <DayOfWeek[]> -Weekly
     [<CommonParameters>]

     New-ScheduledTaskTrigger [-RandomDelay <TimeSpan>] [[-User]
<String>]
     -AtLogOn [<CommonParameters>]

     New-ScheduledTaskTrigger [[-RandomDelay] <TimeSpan>] -AtStartup
     [<CommonParameters>]
```

[illegible]-Daily[illegible]-At[illegible]

```
PS C:\> New-ScheduledTaskTrigger -daily -at 0300

WARNING: column "Enabled" does not fit into the display and was removed
Id     Frequency   Time          DaysOfWeek
--     ---------  ----          ----------
0      Daily     1/1/0001 12:00:00 AM
```

[illegible]

```
PS C:\> New-ScheduledTaskTrigger -daily -at '3:00 am'

WARNING: column "Enabled" does not fit into the display and was
removed.
Id    Frequency    Time         DaysOfWeek
--    ---------    ----         ----------
0     Daily      4/18/2012 3:00:00 AM
```

[illegible]ID[illegible]0[illegible]Get-ScheduledTaskTrigger[illegible]PowerShell[illegible]ID[illegible]

[illegible]

```
PS C:\> help New-ScheduledTaskAction

NAME
    New-ScheduledTaskAction

SYNTAX
     New-ScheduledTaskAction [-Execute] <string> [[-Argument] <string>]
     [[-WorkingDirectory] <string>] [-Id <string>] [-CimSession
     <CimSession[]>] [-ThrottleLimit <int>] [-AsJob]
[<CommonParameters>]
```

[illegible]GUI[illegible]-WorkingDirectory[illegible]-Argument[illegible]-Execute[illegible]

```
PS C:\> New-ScheduledTaskAction -Execute 'dir'

Id                 :
Arguments         :
Execute            : dir
WorkingDirectory :
PSComputerName   :
```

[illegible]

```
PS C:\> New-ScheduledTask -Action (New-ScheduledTaskAction -Execute
'Get-Pr
intJob -printer "Accounting"') -Trigger (New-ScheduledTaskTrigger -
```

```
daily
-at '3:00 am') -Description "Reset accounting printer daily at 3am"
```

[illegible]GUI[illegible]“metro”[illegible]

```
PS C:\> gcm -Module scheduledtasks
Capability   Name
----------    ----
CIM       Get-ClusteredScheduledTask
CIM       Get-ScheduledTask
CIM       Get-ScheduledTaskInfo
CIM       New-ScheduledTask
CIM       New-ScheduledTaskAction
CIM       New-ScheduledTaskPrincipal
CIM       New-ScheduledTaskSettingsSet
Cmdlet, Script  New-ScheduledTaskTrigger
CIM       Register-ClusteredScheduledTask
CIM       Register-ScheduledTask
CIM       Set-ClusteredScheduledTask
CIM       Set-ScheduledTask
CIM       Start-ScheduledTask
CIM       Stop-ScheduledTask
CIM       Unregister-ClusteredScheduledTask
CIM       Unregister-ScheduledTask
```

[illegible]Register-ScheduledTask[illegible]“New”[illegible]“[illegible]”[illegible]register[illegible]Windows[illegible]

```
NAME
    Register-ScheduledTask

SYNTAX
     Register-ScheduledTask [-TaskName] <string> [[-TaskPath] <string>]
     [-Action] <CimInstance#MSFT_TaskAction[]> [[-Trigger]
     <CimInstance#MSFT_TaskTrigger[]>] [[-Settings]
     <CimInstance#MSFT_TaskSettings>] [[-User] <string>] [[-Password]
     <string>] [[-RunLevel] <RunLevelEnum> {Limited | Highest}]
     [[-Description] <string>] [-Force] [-CimSession <CimSession[]>]
     [-ThrottleLimit <int>] [-AsJob] [<CommonParameters>]
```

[illegible]New-ScheduledTask[illegible]-TaskName[illegible]-User[illegible]-Password[illegible]

```
PS C:\> Register-ScheduledTask -TaskName "ResetAccountingPrinter" -
Descript
ion "Resets the Accounting print queue at 3am daily" -Action (New-
Scheduled
TaskAction -Execute 'Get-PrintJob -printer "Accounting"') -Trigger
(New-Sch
eduledTaskTrigger -daily -at '3:00 am')

WARNING: column "State" does not fit into the display and was removed.
TaskPath                  TaskName
--------                  --------
\                     ResetAccountingPrinter
```



□12.1 □□□□□□GUI□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□GUI□□□12.1□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□

12.4 常见误区与注意

这一章中存在很多细节，很多人都会犯错——许多误区需要引起重视。下面是一些常见误区：

- 试图从一个不能接收管道的参数中读取通过管道的数据。对于这一点，请记住，只有你亲自检查参数的帮助文档，才能理解它是否接收管道输入。不要依赖Google搜索出来的结果或是你的猜测，而是要亲自去查看帮助文档。阅读帮助文档可以避免很多错误。
- 进程标识只能以数字的形式被识别，而不能是名称——尽管有时候进程名称可能会被显示出来，但当你尝试传入一个名称时，会出现错误。类似地，很多时候进程的名称是被传递的唯一信息。比如说，空闲进程的ID号为0，就没有办法通过名称来引用它，如果不清楚这点，很容易认为有问题。PowerShell中同样也会有这种情况：某些实体看起来好像完全一样，却有着不同的属性或是类型的问题。
- 如果你在输入一个参数值时感到困惑，请记住：PowerShell会把所有值看作文本字符串，除非有“必须使用括号括起来的表达式”，否则也会被看成“必须被解释的表达式”。在尝试传入一个值之前，请仔细阅读帮助文档，了解参数预期的数据类型，这可以节省大量的时间。
- 时间格式也是另一个常见的误区——许多人在指定时间时会犯错，例如直接指定0300这样的数字格式，而不是使用一个引号括起来的’3:00 am’这样的字符串，或是更清晰的03:00和03:00:00这种格式。
- 认为可以像GUI那样直接点击运行计划任务，使用-Execute参数将会触发该任务。类似Shell这样的命令行对于Windows计划任务——而言并没有直接运行的概念，它完全不同。

以上几点是初学者最常遇到的误区，但是你还会遇到更多类似的问题——不过我们相信你一定能够应对。

12.5 动手实验

注意：对于本次动手实验，你需要运行PowerShell v3或更新版本PowerShell的计算机。

到目前为止，你已经学习了如何在一个命令中完成各种任务了。现在，你可以在不需要帮助的情况下完成下面的任务。

Windows 8和Windows Server 2012中包含了一个用于处理共享的模块。你的任务是在本地机器上创建一个“LABS”的共享，并设置它的共享路径。请确保这个共享文件夹已经存在，并保证NTFS权限对应用户有足够的权限。在设置共享时，请为每个用户设置完全控制/读取权限，任何人都可以通过网络访问这个共享，并设置相应的权限。（提示：你可能需要先找到能够帮你完成这个任务的命令。）

[illegible]13[illegible] [illegible]

[illegible]PowerShell[illegible]Get-Service[illegible]-ComputerName[illegible]-ComputerName[illegible]Cmdlet[illegible]Cmdlet[illegible]PowerShell[illegible]-ComputerName[illegible]

[illegible]PowerShell[illegible]——[illegible]Cmdlet[illegible]-Computer[illegible]Shell[illegible]Remoting[illegible]Cmdlet[illegible]Cmdlet[illegible]

[illegible] [illegible]“[illegible]”[illegible]

13.1 PowerShell[illegible]

[illegible]PowerShell[illegible]Telnet[illegible]Telnet[illegible]SSH[illegible]PowerShell[illegible]Web[illegible]Web Services for Management[illegible]WS-MAN[illegible]

WS-MAN[illegible]HTTP[illegible]HTTPS[illegible]WS-MAN[illegible]Windows[illegible]WinRM[illegible]PowerShell[illegible]WinRM[illegible]Windows Server 2008 R2[illegible]Windows 7[illegible]Windows Server 2012[illegible]WinRM[illegible]PowerShell[illegible]

[illegible]Windows PowerShell[illegible]Cmdlet[illegible]HTTP[illegible]HTTPS[illegible]XML[illegible]PowerShell[illegible]XML[illegible]XML[illegible]XML[illegible]PowerShell[illegible]XML[illegible]XML[illegible]

[illegible]CPU[illegible]

[illegible]

[illegible]

- [illegible]PowerShell[illegible]Windows XP[illegible]PowerShell[illegible]
- [illegible]PowerShell[illegible]Help About_Remote _Troubleshooting[illegible]

[illegible]PowerShell[illegible]localhost[illegible]

13.2 WinRM[illegible]

[illegible]WinRM[illegible]WinRM[illegible]PowerShell[illegible]Windows[illegible]Windows[illegible]Windows XP[illegible]PowerShell[illegible]

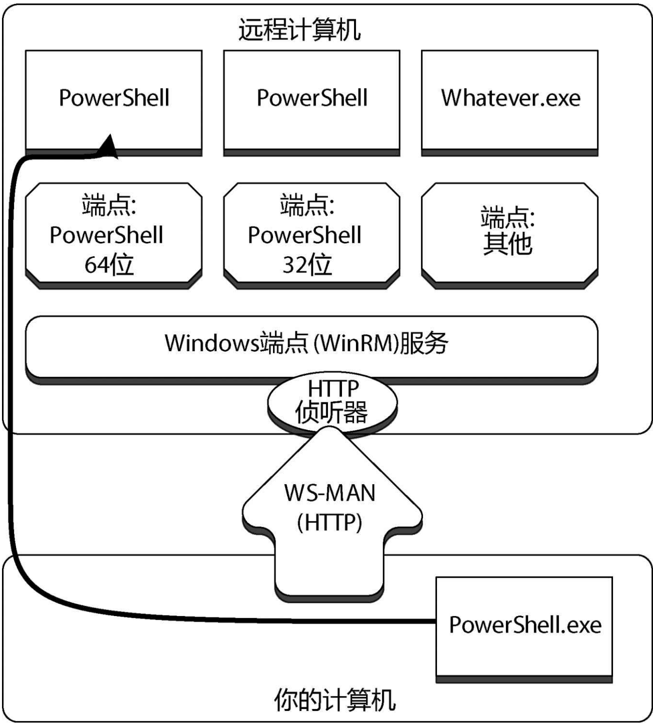
[illegible]PowerShell[illegible]WinRM[illegible]WinRM[illegible]——[illegible]WinRM[illegible]——[illegible]PowerShell[illegible]WinRM[illegible]WinRM[illegible]WinRM[illegible]WinRM[illegible]WinRM[illegible]WinRM[illegible]WinRM[illegible]PowerShell[illegible]13.1[illegible]

[illegible]13.1[illegible]WinRM[illegible]PowerShell[illegible]

□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□23□□□□□□□□□□□□

□13.1□□□□WinRM□□□□□□□□□□□□HTTP□□□□□□□□□□□□□□□WinRM□□
□□□□□□□——□□□Web□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□
□□□□□□□IP□□□□□□□□□□□□□□□□□□□□□□□□IP□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□——□
□□□□□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□□□□□□□□□□□□□□□
□Set-WSManQuickConfig□□□□□□□□□□□□□□□□□Enable-PSRemoting□
□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□Cmdlet□□□WinRM□□□□□□□□□□□□□□□□□□WinRM□□
PowerShell□□□□□□□□□□□□Windows□□□□□□□□□□WinRM□□□□□□□□□□



□13.1 WinRM□WS-MAN□□□□PowerShell□□□□□

□□□
□□□□□□□□□□□□□□□□□□□□□□□PowerShell□PowerShell□□□□□□□□□
□“□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□
□“□□□□□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
Enable-PSRemoting□□□□□□□□□□□□□□□□□□□

□13.2□□□□□□□Enable-PSRemoting□□□□□□□□□□□□□□

□13.2□□□“□□□□”□□□□□□□□Windows Vista□□“□□□□”□□□□□□□□□Windows□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□□□□□□“□□□□”□□“□□□□”□□

```
管理员: Windows PowerShell
PS C:\> enable-psremoting

WinRM 快速配置
正在运行命令“Set-WSManQuickConfig”，以便通过 Windows 远程管理(WinRM)服务对该计算机进行远程管
理。
 其中包括:
    1. 启动或重新启动(如果已启动) WinRM 服务
    2. 将 WinRM 服务启动类型设置为“自动”
    3. 创建侦听程序以接受任意 IP 地址上的请求
    4. 为 WS-Management 通信启用 Windows 防火墙入站规则例外(仅适用于 http)。

是否继续?
[Y] 是(Y)  [A] 全是(A)  [N] 否(N)  [L] 全否(L)  [S] 暂停(S)  [?] 帮助 (默认值为“Y”): y
在此计算机上设置了 WinRM 以接收请求。
Set-WSManQuickConfig : <f:WSManFault xmlns:f="http://schemas.microsoft.com/wbem/wsman/1/wsmanfa
ult"
Code="2150859113" Machine="localhost"><f:Message><f:ProviderFault provider="Config provider"
path="%systemroot%\system32\WsmSvc.dll"><f:WSManFault xmlns:f="http://schemas.microsoft.com/wbe
m/wsman/1/wsmanfault"
Code="2150859113" Machine="                              "><f:Message>由于此计算机上的网络连接类
型之一设置为公用，因此
WinRM 防火墙例外将不运行。 将网络连接类型更改为域或专用，然后再次尝试。
</f:Message></f:WSManFault></f:ProviderFault></f:Message></f:WSManFault>
所在位置 行:116 字符: 17
+                 Set-WSManQuickConfig -force
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Set-WSManQuickConfig], InvalidOperationExc
eption
    + FullyQualifiedErrorId : WsManError,Microsoft.WSMan.Management.SetWSManQuickConfigCommand

PS C:\> _
```

□13.2 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□ □□□

□□GPO□□□□□□□□□□□GPO□□□□□□□□□□Windows Server 2008 R2□□http://download.microsoft.com□□□□□□ADM□Administrative Templates□□□□□□□□□□□□GPO□□□□□□□□□□GPO□□□□□□□□□□□“□□□□□□”>>“□□□□”>>“Windows□□”□□□□□□□□□□□□□□□□□□□□□□□□□“Windows□□□□□

□”□Windows Remote Shell□□“Windows□□□□”□WinRM□□□□□□□□□□□□□□□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□□□□□□□□□□□□□□□

> **□□□** PowerShell□About_Remote_TroubleShooting□□□□□□□□□□□□□□□□GPO□□□□□□□□□□□□□□□□“□□□□□□□□□□□□”□“□□□□□□□□□□□□□□”□□□

□□□□WinRM□□□□□□□□□□□□□PowerShell□□□WinRM□□□□□□□□TCP□□5985□□□HTTP□□□5986□□□□□HTTPS□□□□□□□□□□□□□□□□□□□□Web□□□□□□□□□□□□□□80□443□□□□□□□□□□□□□□Enable-PSRemoting□□□□□□□□□□5985□□□□□□□□HTTP□□□□□□□□□□□□□□WinRM□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□

□□□□□□□□□□□□□□□□□□□□□□□□□□

```
WinRM Set WinRM/Config/Listener?Address=*+Transport=HTTP
➥@{Port="1234"}
```

□□□□□□1234□□□□□□□□□□□□□□□□□□□HTTP□□□HTTPS□□□□□□□□□□HTTPS□□□□□□

□□WinRM□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□WinRM□□WinRM□□□□□□□□□□□□□□□□HTTP□□□□□□□□□□□□HTTPS□□□□□□□□□□□□□□□□IP□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

> **□□□** □□□□□□Windows□□□□□□Remote Shell□□

13.3 □□□□□□Enter-PSSession□Exit-PSSession

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□1:1□□□□□□□□□□□□□□□□□□1 : *n*□□Shell□□

[illegible]Remote Desktop Connection[illegible]Windows PowerShell[illegible]

[illegible]

```
Enter-PSSession –ComputerName Server-R2
```

[illegible]Server-R2[illegible]

[illegible]Shell[illegible]

```
[Sever-R2] PS C:\>
```

[illegible]Shell[illegible]Server-R2[illegible]PSSnapIn[illegible]

[illegible]WinRM[illegible]IP[illegible]DNS[illegible]

[illegible]PowerShell[illegible]Kerberos[illegible]PowerShell[illegible]

[illegible]

- [illegible]PowerShell[illegible]Profile[illegible]Profile[illegible]25[illegible]Profile[illegible]Shell[illegible]Profile[illegible]Shell[illegible]Profile[illegible]
- [illegible]RemoteSigned[illegible]

[illegible]——[illegible]PowerShell[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]Enter-PSSession[illegible]

[illegible]Exit-PSSession[illegible]Shell[illegible]

[illegible]Exit-PSSession[illegible]

[illegible]Exit-PSSession[illegible]PowerShell[illegible]PowerShell[illegible]WinRM[illegible]

[illegible]Enter-PSSession[illegible]Computer A[illegible]Windows 7[illegible]Server-R2[illegible]PowerShell[illegible]

```
[Server-R2] PS C:\>Enter-PSSession Server-DC4
```

[illegible]Server-R2[illegible]Server-DC4[illegible]“[illegible]”[illegible]——[illegible]Server-DC4[illegible]Server-R2[illegible]Server-DC4[illegible]

> [illegible]“[illegible]”[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]23[illegible]

[illegible]Stop-Process[illegible]

13.4 [illegible]Invoke-Command

[illegible]Windows PowerShell[illegible]PowerShell[illegible]Invoke-Command[illegible]1 : *n*[illegible]

[illegible]

```
Invoke-Command –ComputerName Server-R2,Server-DC4,Server12
➥–Command {Get-EventLog Security –Newest 200 |
➥Where {$_.EventID –eq 1212 }}
```

[illegible]

[illegible]{}[illegible]PowerShell[illegible]32[illegible]32[illegible]Invoke-Command[illegible]-ThrottleLimit[illegible]

[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]

```
Invoke-Command –ComputerName Server-R2,Server-DC4,Server12
➥-Command {Get-EventLog Security –Newest 200 |
➥Where { $_.EventID –EQ 1212 }}
```

[illegible]Invoke-Command[illegible]Where[illegible]Where-Object[illegible]Where[illegible]

```
Get-EventLog Security –Newest 200 | Where {$_.EventID –EQ 1212}
```

[illegible]

[illegible]

[illegible]Invoke-Command[illegible]-Command[illegible]-Command[illegible]-ScriptBlock[illegible]Invoke-Command[illegible]-Command[illegible]-Command[illegible]-ScriptCommand[illegible]

[illegible]Invoke-Command[illegible]——[illegible]

[illegible]Invoke-Command[illegible]-ScriptBlock[illegible]-FilePath[illegible]

[illegible]-ComputerName[illegible]Invoke-Command[illegible]Web[illegible]——[illegible]PowerShell[illegible]

```
Invoke-Command –Command {dir}
➥–ComputerName (Get-Content WebServers.txt)
```

[illegible]PowerShell[illegible]Get-Content[illegible]——[illegible]Get-[illegible]-ComputerName[illegible]

[illegible]Get-ADComputer[illegible]Windows 7[illegible]（RSAT）/Windows Server 2008 R2[illegible]Get-Content[illegible]Get-Content[illegible]-Computer[illegible]String[illegible]Get-ADComputer[illegible]-ComputerName[illegible]

[illegible]Get-ADComputer[illegible]

```
Invoke-Command –Command {dir} –ComputerName (
➥Get-ADComputer –Filter * -SearchBase "OU=Sales,DC=Company,DC=pri" |
➥Select-Object –Expand Name)
```

[illegible]Windows Server 2008 R2[illegible]RSAT[illegible]Windows 7[illegible]PowerShell[illegible]Import-Module ActiveDirectory[illegible]Sales OU[illegible]OU=Sales[illegible]OU=Domain Controllers[illegible]Company[illegible]Pri[illegible]mycompany.org[illegible]mycompany[illegible]company[illegible]org[illegible]pri[illegible]

[illegible]Select-Object[illegible]-Expand[illegible]Name[illegible]——[illegible]-ComputerName[illegible]

[illegible] [illegible]-Expand[illegible]9[illegible]9[illegible]
[illegible]

[illegible]Get-ADComputer[illegible]-Filter[illegible]-SearchBase[illegible]——[illegible]Company.Pri[illegible]Sales OU[illegible]Get-ADComputer[illegible]Windows Server 2008 R2[illegible]RSAT[illegible]Windows 7[illegible]

13.5 [illegible]

[illegible]Invoke-Command[illegible]

```
Invoke-Command –ComputerName Server-R2,Server-DC4,Server12
➥-Command {Get-EventLog Security –Newest 200 |
➥Where {$_.EventID –EQ 1212}}
```

[illegible]

13.5.1 Invoke-Command VS –ComputerName

[illegible]

```
Get-EventLog Security–Newest 200
➥–ComputerName Server-R2,Server-DC4,Server12 |
➥Where {$_.EventID -EQ 1212}
```

[illegible]Get-EventLog[illegible]-ComputerName[illegible]

- [illegible]
- [illegible]PSComputerName[illegible]
- [illegible]WinRM[illegible].Net FrameWork[illegible]
- [illegible]3[illegible]200[illegible]eventid[illegible]1212[illegible]
- [illegible]

□□□-ComputerName□□□Cmdlet□□□□□□□□□□□□□□□□□□Invoke-Command□□□Cmdlet□-ComputerName□□□□□□□□□□□□

□□□□□□□□□□Invoke-Command□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□PSComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□WinRM□□□□□□□WinRM□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□200□□□
- □□□□□□□□□□□□□□□□□□□□□□□□□□XML□□□□□□□□□□XML□□

□□□□□□□-ComputerName□□□Invoke-Command□□□□□□□□□□□□□□□□□□□□□□□□□

13.5.2 □□□□VS□□□□

□□□□□□□□□□□

```
Invoke-Command–ComputerName Server-R2,Sever-DC4,Server12
➡-Command {Get-EventLog Security –Newest 200 |
➡Where {$_.EventID –EQ 1212}}
```

□□□□□□□□□□□□□□

```
Invoke-Command –ComputerName Server-R2,Server-DC4,Server12
➡-Command {Get-EventLog Security –Newest 200 } |
➡Where {$_.EventID –EQ 1212}
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□Get-EventLog□□□□□□□□□Get-EventLog□□Where□□□3□□□□□□□□□□□□□□□□□3□□

□□□□□□□□□□□□□□□□□□□□□□□□

```
Invoke-Command –ComputerName Server-R2
➡-Command {Get-Process –Name Notepad}|
➡Stop-Process
```

[illegible]

```
Invoke-Command –ComputerName Server-R2
➡-Command {Get-Process –Name NotePad |
➡Stop-Process}
```

[illegible]

[illegible]Get-Process-Name NotePad[illegible]XML[illegible]XML[illegible]Stop-Process[illegible]XML[illegible]NotePad[illegible]

[illegible]Invoke-Command[illegible] Get-Process-Name Notepad | Stop-Process[illegible]Stop-Process[illegible]NotePad[illegible]Notepad[illegible]

[illegible]Invoke-Command[illegible]PowerShell[illegible]Invoke-Command[illegible]Invoke-Command[illegible]Cmdlet[illegible]

13.5.3 [illegible]

[illegible]Method[illegible]

[illegible]Service-Controller[illegible]

```
PS C:\>Get-Service | Get-Member

    TypeName: System.ServiceProcess.ServiceController
Name            MemberType    Definition
----            ----------    ----------
Name            AliasProperty  Name = ServiceName
```

```
RequiredServices     AliasProperty  RequiredServices = ServicesDep
Disposed         Event     System.EventHandler Disposed(S
Close          Method     System.Void Close()
Continue         Method     System.Void Continue()
CreateObjRef       Method     System.Runtime.Remoting.ObjRef
Dispose         Method     System.Void Dispose()
Equals          Method     bool Equals(System.Object obj)
ExecuteCommand      Method     System.Void ExecuteCommand(int
GetHashCode        Method     int GetHashCode()
GetLifetimeService    Method     System.Object GetLifetimeServi
GetType         Method     type GetType()
InitializeLifetimeService Method     System.Object InitializeLifeti
Pause          Method     System.Void Pause()
Refresh         Method     System.Void Refresh()
Start          Method     System.Void Start(), System.Vo
Stop           Method     System.Void Stop()
WaitForStatus       Method     System.Void WaitForStatus(Syst
CanPauseAndContinue    Property    bool CanPauseAndContinue {get;
CanShutdown        Property    bool CanShutdown {get;}
CanStop         Property    bool CanStop {get;}
Container        Property    System.ComponentModel.IContain
DependentServices     Property    System.ServiceProcess.ServiceC
```

□□□□□□□□□□□□□□□□

```
PS C:\> Invoke-Command -ScriptBlock { Get-Service } -ComputerName
      WCMIS034 | Get-Member

    TypeName: Deserialized.System.ServiceProcess.ServiceController
Name        MemberType    Definition
----        ----------    ----------
ToString      Method      string ToString(), string ToString(string
       format, System.I
Name        NoteProperty    System.String Name=AeLookupSvc
PSComputerName    NoteProperty    System.String
PSComputerName=WCMIS034
PSShowComputerName  NoteProperty    System.Boolean
PSShowComputerName=True
RequiredServices   NoteProperty
       Deserialized.System.ServiceProcess.ServiceController[] Req
RunspaceId     NoteProperty    System.Guid RunspaceId=6dc9e130-f7b2-
4db4-
       8b0d-3863033d7df
CanPauseAndContinue  Property     System.Boolean {get;set;}
CanShutdown     Property     System.Boolean {get;set;}
CanStop       Property     System.Boolean {get;set;}
Container      Property       {get;set;}
DependentServices  Property
       Deserialized.System.ServiceProcess.ServiceController[] {ge
DisplayName     Property     System.String {get;set;}
```

```
MachineName     Property     System.String {get;set;}
ServiceHandle    Property     System.String {get;set;}
ServiceName     Property     System.String {get;set;}
ServicesDependedOn  Property
       Deserialized.System.ServiceProcess.ServiceController[] {ge
ServiceType     Property     System.String {get;set;}
Site        Property       {get;set;}
Status       Property     System.String {get;set;}
```

[illegible]ToString()[illegible]

13.6 [illegible]

[illegible]20[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]RDP[illegible]RDP[illegible]PowerShell[illegible]PowerShell[illegible]RDP[illegible]RDP[illegible]PowerShell[illegible]

13.7 [illegible]

[illegible]Invoke-Command[illegible]Enter-PSSession[illegible]-SessionOption[illegible]PSSessionOption[illegible]

[illegible]PowerShell[illegible]Session Option[illegible]New-PSSessionOption[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]SSL[illegible]

[illegible]

```
PS C:\> Enter-PSSession –ComputerName Wcmis034
➥–SessionOption (New-PSSessionOption –SkipCNCheck)
[WCMIS034] : PS C:\Users\wh42\Documents>
```

[illegible]New-PSSessionOption[illegible]20[illegible]

13.8 [illegible]

[illegible]

- [illegible]DNS[illegible]IP[illegible]23[illegible]
- [illegible]About*Remote*TroubleShooting[illegible]PowerShell[illegible]
- [illegible]PowerShell[illegible]PowerShell[illegible]
- [illegible]PowerShell[illegible]UAC[illegible]Enter-PSSession[illegible]Invoke-Command[illegible]-Credential[illegible]
- [illegible]Windows[illegible]Enable-PSRemoting[illegible]
- [illegible]GPO[illegible]GPO[illegible]GPO[illegible]GPO[illegible]

13.9 [illegible]

> **[illegible]** [illegible]PowerShell v3[illegible]

[illegible]

1[illegible]localhost[illegible]NotePad.exe[illegible]

2[illegible]Invoke-Command[illegible]localhost[illegible]——[illegible]Format- Cmdlet[illegible]

3[illegible]Invoke-Command[illegible]10[illegible]localhost[illegible]

4[illegible]localhost[illegible]Invoke-Command[illegible]100[illegible]

13.10 [illegible]

[illegible]PowerShell[illegible]http://PowerShellBooks.com [illegible]Don[illegible]MVP Dr. Tobias Weltner[illegible]PowerShell[illegible]Step-by-step[illegible]http://bit.ly/AskDon [illegible]Don[illegible]

□14□ Windows□□□

□□□□□□□□□□□□□□Windows□□□□Windows Management Instrumentation□WMI□□□ WMI□□□PowerShell□□□□WMI□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□WMI□□□□□□□PowerShell□□□□□□□□□□□□□□□□□PowerShell□□□WMI□□□□□WMI□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□WMI□□□□□□□□□□

14.1 WMI□□

□□□Windows□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□

□□□□WMI□□□□□□□□namespaces□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“root\CIMv2”□□□□□□□□□Windows□□□□□□□□□□□□□“root\MicrosoftDNS”□□□□□□□□□□DNS□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“root\SecurityCenter”□□□□□□□□□□□□□□□□□□□□□□□

> □□□ “root\SecurtityCenter”□□□□□□□□□□□□□□□□□□□□□□□□Windows□□“root\SecurityCenter2”□□□□□□□WMI□□□□□□

□14.1□□□□□□□□□□Microsoft Management Console□MMC□□WMI□□□□□□□□□□□□□□□□□

□□□□□□WMI□□□□□□□□□□□□□□WMI□□□□□□□□□□□“root\SecurityCenter”□□“Antivirus-Product”□□□□□□□□□□□□□□□□“root\CIMv2”□□“Win32_LogicalDisk”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Win32_TapeDrive”□□□□Windows□□□□□□□□□□□□□□□□□□



□14.1 □□WMI□□□□

□□□ □□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□Windows□□“Root\SecurityCenter2”□□□□□□□□“Root\SecurityCenter”□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□“root\SecurityCenter2”□□□“AntiSpywareProduct”□□□□□□□□□□□

```
PS C:\> Get-CimInstance -Namespace root\securitycenter2 -ClassName
antispyw
areproduct
```

□□□ □□□□PowerShell v3□□□□□□□□□□□□□□“Get-CimInstance”□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□instances□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□BIOS□□□□“root\CIMv2”□□□□□□□“Win32_BIOS”□□□□□□□□□□□□□100□□□□□□□□□□100□“Win32_Service”□□□□□□□□□□“root\CIMv2”□□□□□□□“Wim32_”□□□□

64□□□□□□□□□“CIM_”□Common Information Model□□□□□WMI□□□□□□□
□□
WMI□□□
WMI□□□

□□□□□□□□□□□□□□□□□□□□□□□WMI□□□WMI repository□□□□□□□□
Windows□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Win 7□□□□□□□□□□□□
□□

□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□
□□action□□□□□□□□□□□
□configuration change□□

14.2 □□WMI□□□□

WMI□□WMI□
□□□WMI□□□□□

□“root\CIMv2”□□□□□□□□□□□□□□□□□□□□□□□□□□□methods□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□IIS□□□□
WMI□IIS□□□
□□IIS□□□□□□□
□□□□□□□□□□IIS□□□□□□□□□WMI□□□□□□□□□□□□□v7.5□□□□□□□□□□
PowerShell Cmdlets□□□□□□□□PSProvider□□□WMI□

□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□WMI□□□□□□WMI□□□□□□□□
□□□□□□DHCP□□□□□□□□WMI□□□□□□□□Windows□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□“Win32_”□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□PowerShell Cmdlets□□□□□□□□□□□□□□□□
□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□“Win32_OperatingSystem”□□□□□□□□PowerShell□□□□□□□“Restart-
Computer”□Cmdlet□□□□□□□□□□□□Cmdlets□□□□□WMI□□□□□□□□□□□
WMI□Cmdlets□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□
□□□□□□□□□□□□□□□ □WMI□

□□□□□PowerShell v3□□□□□□□□□□□□□□“CIM”□□□□□14.2□□□□□“Get-Command”□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□PowerShell□□□□WMI□□□□□□□□□□□□□□Cmdlet□□□□□□Cmdlet□□□□□□Cmdlet□□Help□□□□□□□□□□Cmdlet□□□□□PowerShell□□Cmdlet□□□□□□□□□□□□□□□□□□WMI□□□□□

14.3 □□WMI

□□□WMI□□□□□□□□□PowerShell□□WMI□□□□□□□□□□□□□□□SAPIEN Technologies□□□http://www.sapien.com/downloads □□□□□□□□□□□□□WMI□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□U□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□WMI□□□

```
管理员: Windows PowerShell
PS E:\WINDOWS\system32> gcm

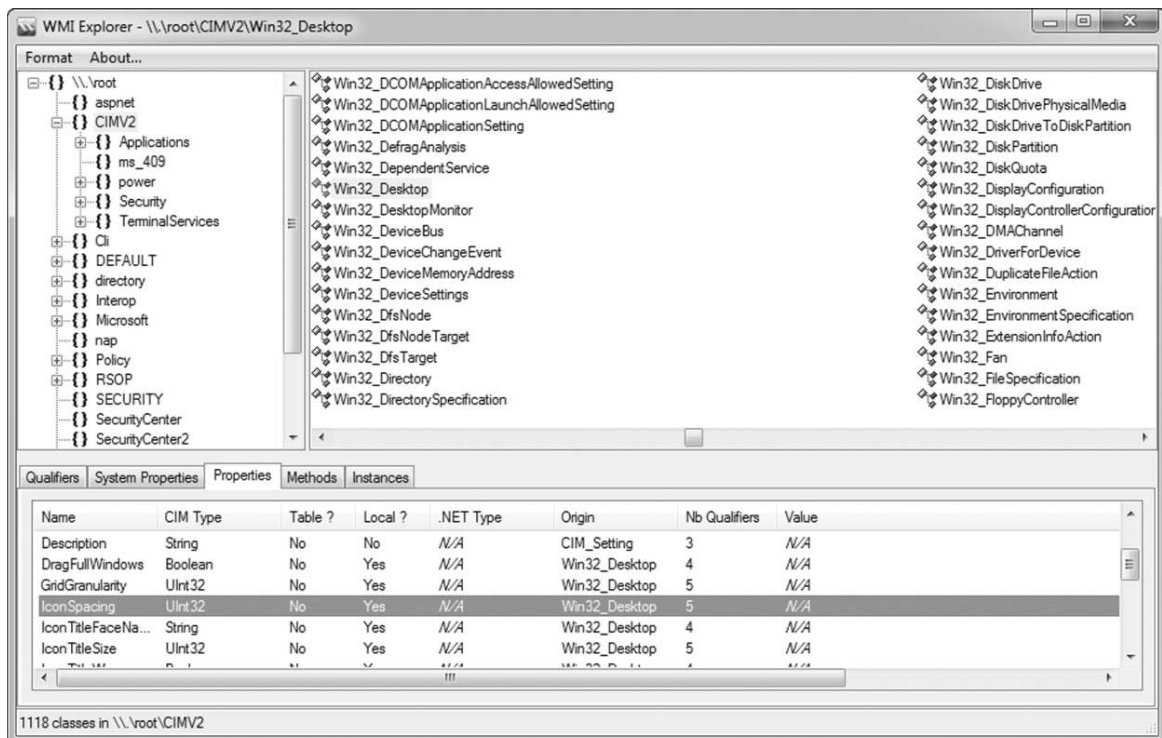
CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Alias           Add-ProvisionedAppxPackage                         Dism
Alias           Apply-WindowsUnattend                              Dism
Alias           Begin-WebCommitDelay                               WebAdminis
Alias           End-WebCommitDelay                                 WebAdminis
Alias           Flush-Volume                                       Storage
Alias           Get-PhysicalDiskSNV                                Storage
Alias           Get-ProvisionedAppxPackage                         Dism
Alias           Initialize-Volume                                  Storage
Alias           Move-SmbClient                                     SmbWitness
Alias           Remove-ProvisionedAppxPackage                      Dism
Alias           Write-FileSystemCache                              Storage
Function        A:
Function        Add-BCDataCacheExtension                           BranchCach
Function        Add-BitLockerKeyProtector                          BitLocker
Function        Add-DnsClientNrptRule                              DnsClient
Function        Add-DtcClusterTMMapping                            MsDtc
Function        Add-InitiatorIdToMaskingSet                        Storage
Function        Add-MpPreference                                   Defender
Function        Add-NetEventNetworkAdapter                         NetEventPa
Function        Add-NetEventPacketCaptureProvider                  NetEventPa
Function        Add-NetEventProvider                               NetEventPa
Function        Add-NetEventVmNetworkAdapter                       NetEventPa
Function        Add-NetEventVmSwitch                               NetEventPa
Function        Add-NetIPHttpsCertBinding                          NetworkTra
Function        Add-NetLbfoTeamMember                              NetLbfo
Function        Add-NetLbfoTeamNic                                 NetLbfo
Function        Add-NetNatExternalAddress                          NetNat
Function        Add-NetNatStaticMapping                            NetNat
Function        Add-NetSwitchTeamMember                            NetSwitchT
Function        Add-OdbcDsn                                        Wdac
Function        Add-PartitionAccessPath                            Storage
Function        Add-PhysicalDisk                                   Storage
Function        Add-Printer                                        PrintManag
```

□14.2 “CIM”□□□WMI□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□□□□□□□□□□□“root\CIMv2”□□□□□WMI□□□□□□□□□□14.3□□□□□□□□□□□□□□□□□□□“Desktop”□□□□□□□□□□□□□□□□□“Win32_Desktop”□□“IconSpacing”□□□□□

□□□□□□□□□□□□□□□□□□□□□□□“WMI”□□“WMI□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□VBScript□□□□□□□C#□Visual Basic□.NET□□□□□□□□□□□□□□□□WMI□□□□ □□□□□□□□□□□□Google□□□“wmi icon spacing”□□□□□□
http://stackoverflow.com/questions/202971/formula-or-api-for-calulating-desktop-icon-spacing-on-windows-xp □□□□□□□□□□□□□□□C#□□□

```
ManagementObjectSearcher searcher = new
      ManagementObjectSearcher("root\\CIMV2"□"SELECT * FROM
Win32_Desktop");
```



□14.3 WMI□□□

□□□□□□□□□□□□“Win32_Desktop”□□

□□□□□□□□□□PowerShell□□“root\CIMv2”□□□□□OS□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> Get-WmiObject -Namespace root\CIMv2 -list | where name -like
'*dis *'

     NameSpace:ROOT\CIMv2
Name                            Methods         Properties
----                                        -------           ----------
Win32_DisplayConfiguration           {}          {BitsPerPel□
Caption□...}
Win32_DisplayControllerConfigura... {}          {BitsPerPixel□
Caption□...}
CIM_DiskSpaceCheck                  {Invoke}            ...}
CIM_DiscreteSensor                  {SetPowerState□ R...
{AcceptableValues□ Availability□...
CIM_Display                  {SetPowerState□ R... {Availability□
Caption□...
CIM_DiskDrive                        {SetPowerState□ R...
{Availability□ Capabilities□...
Win32_DiskDrive                       {SetPowerState□ R...
{Availability□ BytesPerSector□...
CIM_DisketteDrive                     {SetPowerState□ R...
{Availability□ Capabilities□...
CIM_LogicalDisk                         {SetPowerState□ R... {Access□
Availability□ BlockSize□...}
Win32_LogicalDisk                       {SetPowerState□  R... {Access□
Availability□ BlockSize□...}
Win32_MappedLogicalDisk                {SetPowerState□ R...  {Access□
Availability□ BlockSize□...}
CIM_DiskPartition                        {SetPowerState□ R...  {Access□
Availability□ BlockSize□...}
Win32_DiskPartition                    {SetPowerState□ R...  {Access□
Availability□ BlockSize□...}
Win32_LogicalDiskRootDirectory       {}          {GroupComponent□
PartComponent}...
Win32_DiskQuota             {}         {DiskSpaceUsed□ Limit□...}
Win32_LogonSessionMappedDisk        {}          {Antecedent□
Dependent}...
CIM_LogicalDiskBasedOnPartition      {}          {Antecedent□
Dependent□...
Win32_LogicalDiskToPartition         {}          {Antecedent□
Dependent□...
CIM_LogicalDiskBasedOnVolumeSet      {}          {Antecedent□
Dependent□...
Win32_DiskDrivePhysicalMedia         {}          {Antecedent□
Dependent}...
CIM_RealizesDiskPartition              {}          {Antecedent□
Dependent□...
```

```
Win32_DiskDriveToDiskPartition       {}         {Antecedent□ Dependent}
Win32_OfflineFilesDiskSpaceLimit     {}         {AutoCacheSizeInMB□...
Win32_PerfFormattedData_Counters...  {}         {Caption□
Description□...
Win32_PerfRawData_Counters_FileS...  {}         {Caption□
Description□...
Win32_PerfFormattedData_Distribu...  {}
{AckMessagesReceivedPersecond□...
Win32_PerfRawData_DistributedRou...  {}
{AckMessagesReceivedPersecond□...
Win32_PerfFormattedData_MSDTC_Di... {}         {AbortedTransactions□...
Win32_PerfRawData_MSDTC_Distribu... {}         {AbortedTransactions□
Win32_PerfFormattedData_MSSQLSER...  {}         {Caption□
Description□...
Win32_PerfRawData_MSSQLSERVER_SQ... {}         {Caption□
Description□...
Win32_PerfFormattedData_PeerDist... {}         {BITSBytesfromcache□...
Win32_PerfRawData_PeerDistSvc_Br... {}         {BITSBytesfromcache□...
Win32_PerfFormattedData_PerfDisk... {}         {AvgDiskBytesPerRead□...
Win32_PerfRawData_PerfDisk_Logic... {}         {AvgDiskBytesPerRead□...
Win32_PerfFormattedData_PerfDisk... {}         {AvgDiskBytesPerRead□...
Win32_PerfRawData_PerfDisk_Physi... {}         {AvgDiskBytesPerRead□...
```

□□□□□□“Win32_LogicalDisk”□

□□□ □□□“CIM”□□□□□□□□□□□□□□□□□□□□“Win32”□□□□□Windows□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□

14.4 □□□□□□□WMI□CIM

□PowerShell v3□□□□□□□□□□WMI□□□□□□

- □□□“WMI Cmdlets”□□“Get-WmiObject”□“Invoke-WmiMethod”——□□□RPC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□“CIM Cmdlets”□□“Get-CimInstance”□“Invoke-CimMethod”——□□□□□□□□□□□□“WMI Cmdlets”□□□□□□WS-MAN□□Windows□□□□□□□□□□□□□□□□RPCs□□□□□□□□□□□□“Get-Command–noun CIM*”□□□□□□□□□□□□□□□ □□□

□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□Windows □□□□□□□□□□WMI Cmdlets□□□□□□□□□□

Windows NT 4.0 SP3□□□□□□□□□□□□PowerShell□□□□Windows□□□□□□□□□□□CIM Cmdlets□□□□□□——□□□□□□□□□□□□□□□□□□□□

14.5 □□Get-WmiObject

□□“Get-WmiObject” Cmdlet□□

□□

```
Get-WmiObject -namespace root\cimv2 –list
```

□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□

```
Get-WmiObject -namespace root\cimv2 -class win32_desktop
```

□□“root\CIMv2”□□□□Windows XP SP2□□“-class”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□Gwmi□□□□□□□Cmdlet□□

```
PS C:\> Get-WmiObject win32_desktop
PS C:\> gwmi antispywareproduct -namespace root\securitycenter2
```

□□□localhost□□□

□□□□WMI□□PowerShell□□□□□□□□□□□□□□□□□□□
□□“Win32_OperatingSystem”□□□□□□□□□□□□□□□□□□□□□□□6□□□□□□
□□□□□□□WMI□□□□□□□“Gm”□“Format-List *”□□□□□□□□□□□□
□□“Gm”□□□□□□□□□□□□□□□□□□

```
PS C:\> Get-WmiObject win32_operatingsystem | gm

   TypeName:
System.Management.ManagementObject#root\cimv2\Win32_Operating
```

```
System

Name                       MemberType  Definition
----                       ----------  ----------
Reboot                          Method      System.Managemen...
SetDateTime                   Method      System.Managemen...
Shutdown                        Method      System.Managemen...
Win32Shutdown                  Method      System.Managemen...
Win32ShutdownTracker        Method      System.Managemen...
BootDevice                      Property    System.String Bo...
BuildNumber                     Property    System.String Bu...
BuildType                       Property   System.String Bu...
Caption                          Property    System.String Ca...
CodeSet                         Property     System.String Co...
CountryCode                     Property    System.String Co...
CreationClassName               Property     System.String Cr...
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□“-filter”□□

```
PS C:\> gwmi -class win32_desktop -filter
"name='COMPANY\\Administrator'"

__GENUS                  : 2
__CLASS                  : Win32_Desktop
__SUPERCLASS            : CIM_Setting
__DYNASTY                : CIM_Setting
__RELPATH                : Win32_Desktop.Name="COMPANY\\Administrator"
__PROPERTY_COUNT        : 21
__DERIVATION            : {CIM_Setting}
__SERVER                 : SERVER-R2
__NAMESPACE           : root\cimv2
__PATH                : \\SERVER-
R2\root\cimv2:Win32_Desktop.Name="COMPANY
                        \\Administrator"
BorderWidth           : 1
Caption                 :
CoolSwitch              :
CursorBlinkRate       : 530
Description             :
DragFullWindows        : False
GridGranularity         :
IconSpacing             : 43
IconTitleFaceName       : Tahoma
IconTitleSize           : 8
IconTitleWrap           : True
Name                    : COMPANY\Administrator
```

```
Pattern                : 0
ScreenSaverActive    : False
ScreenSaverExecutable :
ScreenSaverSecure     :
ScreenSaverTimeout    :
SettingID             :
Wallpaper              :
WallpaperStretched    : True
WallpaperTiled         : False
```

[illegible]

- [illegible]
- [illegible]PowerShell[illegible]“-eq”[illegible]“-like”[illegible]=[illegible]>[illegible]<[illegible]<=[illegible]>=[illegible]<>[illegible]“LIKE”[illegible]“%”[illegible]“NAME LIKE ‘%administrator%’”[illegible]PowerShell[illegible]*[illegible]
- [illegible]
- [illegible]WMI[illegible]
- Gwmi[illegible]PowerShell[illegible]

__SERVER[illegible]WMI[illegible]“PSComputerName”[illegible]
__PATH[illegible]

[illegible]Cmdlet[illegible]IP[illegible]

```
PS C:\> Gwmi Win32_BIOS -comp server-r2,server3,dc4
```

[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]30[illegible]45[illegible]

[illegible]WMI[illegible]“-Object”Cmdlet[illegible]“Format-”Cmdlet[illegible]“Out-”[illegible]“Export-”[illegible]“ConvertTo-”Cmdlet[illegible]“Win32_BIOS”[illegible]

```
PS C:\> Gwmi Win32_BIOS | Format-Table SerialNumber□Version –auto
```

□□10□□□□□□□□□□□□□□“Format-Table”Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> gwmi -class win32_bios -computer server-r2□localhost | format-
table
 @{l='ComputerName';e={$_.__SERVER}}□@{l='BIOSSerial';e=
{$_.SerialNumber}}□
@{l='OSBuild';e={gwmi -class win32_operatingsystem -comp $_.__SERVER |
sele
ct-object -expand BuildNumber}} -autosize

ComputerName BIOSSerial                                     OSBuild
------------ ----------                                       --------
SERVER-R2    VMware-56 4d 45 fc 13 92 de c3-93 5c 40 6b 47 bb 5b 86
7600
```

□□□□□□□□□□□□□PowerShell ISE□□□□□□□□□□□□□□□□

```
gwmi -class win32_bios -computer server-r2□localhost |
 format-table
  @{l='ComputerName';e={$_.__SERVER}}□
  @{l='BIOSSerial';e={$_.SerialNumber}}□
  @{l='OSBuild';e={
    gwmi -class win32_operatingsystem -comp $_.__SERVER |
    select-object -expand BuildNumber}
  } –autosize
```

□□□□□□

- “Get-WmiObject”□□□□□□□□□□□“Win32_BIOS”□□□
- □□□□□□□□□□“Format-Table”□“Format-Table”□□□□□□□□□□□□□
  □□□□□□□□ComputerName□□□“Win32_BIOS”□□□□“__SERVER”□□□□□□□
  □□□□□□□□BIOSSerial□□□“Win32_BIOS”□□□□“SerialNumber”□□□□□
  □□□□□□□□OSBuild□□□□□□□□□□□“Get-WmiObject”□□□□“Win32_BIOS”□□□□“__SERVER”□□□□□“Win32_OperatingSystem”□□□□□□□□□□□□□□□“Select-Object”□□□□□□□□□□“Win32_OperatingSystem”□□□□“BuildNumber”□□□□□□□□□□OSBuild□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
PowerShell Cmdlet□□□□□□□

□□□□□□□□WMI□□□□□□□□□16□□□□□□□□□□□□□□□□□□□□
□□□□□□□

14.6 □□Get-CimInstance

Get-CimInstance□PowerShell v3□□□□□□“Get-WmiObject”□□
□□□□□□□□□□□□□□□□

- □□□□“-ClassName”□□“-Class”□□□□□□□-Class□□□□□□□□□□
  □□□□□□□□□□□
- □□□□□□□□□□□□□□“-List”□□□□□□□□□“Get-CimClass”□□“-Namespace”□□□□□□□
- □□“-Credential”□□□□□□□□□□□□□□□□□□□□□□□□□“Invoke-Command”□□□□□□□□□“Get-CimInstance”□□□

```
PS C:\> Get-CimInstance -ClassName Win32_LogicalDisk

DeviceID   DriveType ProviderName     VolumeName        Size
FreeSpace
--------   ---------  -----------     ----------       ----        ----
-----
A:          2
C:          3                                                 687173...
580806...
D:          5                              HB1_CCPA_X64F... 358370...
0
```

□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> invoke-command -ScriptBlock { Get-CimInstance -ClassName
win32_proc
ess } -ComputerName WIN8 -Credential DOMAIN\Administrator
```

14.7 WMI□□

□□□□□□□□□□□□□□WMI□□□□□□□“Win32_”□□□□MSDN□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Google□Bing□□
□□□□□□□□□□http://msdn.microsoft.com/ □

14.8 □□□□

□□□□10□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□PowerShell□
□□□□“help win32_service”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□
□□□□PowerShell□□
□□□□□□□□□□□□□□□□□□□□□□“root\SecurityCenter”□□□□□□□□□□□□□□□□
□□□□□□□□□□

WMI□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□PowerShell□□□□□□□□□□□
WMI□□□□□□□□□□□□PowerShell□□□□

□□□□□□□□□□□□□□□□□WMI□□□□□□□PowerShell□□□□WMI□□□□□□□□□
□□□□WMI□□□□□PowerShell□□WMI□□□□□□□□□□□□□□□□□□□□□WMI□□□
□□PowerShell□□□□□□□□□Cmdlets□□□□□□□□Cmdlets□□□□□
PowerShell□□□□□□□WMI□□□□□□

14.9 □□□□



□□□□□□□□□□□□□□□□PowerShell v3□□□□□PowerShell□□□

□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□WMI explorer□□
□□□□□□WMI Explorer□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□
□□□□□□□□□□□□WMI□□

1□□□□□□□□□□□□□□□□□□IP□□□□□□□□□□□□□□□□□□DHCP□□□□□□□
network□□□□□□□□□□□□

2□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□BIOS□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□OS□□□□□□BIOS□□

3□□□WMI□□□□□□□□□□hotfixes□□□□□□□□□□□□□□□□□□□□quick fix
engineering□□□□□□□□□□□□□“Get-Hotfix”□□□□□□□

4□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

5[illegible]

[illegible]2[illegible]

14.10 [illegible]

WMI[illegible] PowerShell and WMI by fellow MVP Richard Siddaway(Manning[illegible] 2012)[illegible]PowerShell v3[illegible]CIM Cmdlets[illegible]WMI[illegible]

[illegible]WMI[illegible]PowerShell v3[illegible]WMI[illegible]Cmdlets[illegible]WMI[illegible]Cmdlets[illegible]Cmdlets[illegible]WMI[illegible]WMI[illegible]

[illegible]15[illegible] [illegible]

[illegible]“[illegible]”[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]13[illegible]14[illegible]WMI[illegible]

15.1 [illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]

15.2 [illegible]VS[illegible]

[illegible]PowerShell[illegible]_[illegible]_[illegible]_[illegible]_[illegible]PowerShell[illegible]

[illegible]

- [illegible]——[illegible]
- [illegible]22[illegible]
- [illegible]PowerShell[illegible]

PowerShell _Jobs_

PowerShell Scheduled Jobs Shell PowerShell

15.3

Start-Job -ScriptBlock PowerShell Job1 Job2 -Name -Credential \ DOMAIN\UserName -FilePath

```
PS C:\> Start-Job -ScriptBlock {Dir}

Id       Name     PSJobTypeName  State  HasMoreData   Location
---      -----     ------------  ------  -----------  ------------
```

```
-
1       Job1    BackgroundJob  Running True      localhost
```

□□ID□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□-ComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> Start-Job -ScriptBlock {
➥Get-EventLogSecurity -Computer Server-R2
}
Id      Name    PSJobTypeName    State  HasMoreData   Location
---     -----   --------------   ------  -----------  -----------
3     Job3    BackgroundJob    Running True      localhost
```

□□localhost□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Server-R2□□□□□□□□□□□□□□□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□Job1□□□ID□1□□□□□□□Job□□Job3□□□ID□3□□□□□□□□□□□□□□□□□□□□□□□□Job1□□□□□□□□□Job2□□ID□2□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□13□□□□□□□□□□□□□□□□□□□□□□□□□□□□

15.4 WMI□□

□□□□□□□□□□□Get-WMIObject□□□□□□□□□□□□□Get-WMIObject□□

□□□□□□□□□□□□Get-WMIObject□□□□□□□□-AsJob□□□□□□□□□□ □□□□□□□□□□□□□PowerShell□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□C:□□□□□□□□ allservers.txt□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□localhost□□□□ □□□□□□□□□□

```
PS C:\> Get-WMIObject Win32_OperatingSystem -ComputerName (
➥Get-Content allservers.txt) -AsJob

Id    Name    PSJobTypeName  State   HasMoreData   Location
--    ------   ------------  -------  -----------  -----------
5    Job5    WmiJob     Running  True      Server-R2,lo...
```

□□□□□PowerShell□□□□□□□□□□Job5□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□Location□□□□□□□□□□□ □□□□□□□□□□□□□□□□

□□□Get-WMIObject□□□□□□□□□□□□□□□□□□□□□□□□WMI□ □□ □□□□□□□□□□□□□□□□□□Get-WMIObject□□□□□□□□□□□□□□□□

□□□□□□□□□□□Get-WMIObject□□□□□□□□□□□□□□□□ Help * -Parameter AsJob□□□□□□□□□□□□□□□□

□□□□□14□□□□□□Get-CimInstance□□□□□□□-AsJob□□□□□ □□□□□□□□□□□□Start-Job□Invoke-Command□□□□□□□□□□□ □Get-CIMInstance□□□□□□□□CIM□□□□□□□□□

15.5 □□□□□

□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□13□□ □□□□□□□□Get-WMIObject□□□□□□-AsJob□□□□□□□□□□□□□□□□ □□□□□Invoke-Command Cmdlet□□□□

□□□□□□□□□□□-ScriptBlock□□□□□□□□□□□-Command□□□ □□□□□□□□□□□□□□□□□□□□□32□□□□□□□□□□□□□□□-

ThrottleLimit[illegible]32[illegible]32[illegible]32[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]-JobName[illegible]

```
PS C:\> Invoke-Command -Command {Get-Process}
➥–ComputerName (Get-Content .\allservers.txt )
➥-AsJob -JobName MyRemoteJob

Id     Name    PSJobTypeName  State  HasMoreData   Location
---    ----    -------------  -----  ------------  -----------
9     MyRemoteJob RemoteJob   Running True      Server-R2,loca...
```

15.6 [illegible]

[illegible]Get-Job Cmdlet[illegible]

```
PS C:\> Get-Job

Id   Name     PSJobTypeName  State   HasMoreData  Location
---  ----     -------------  -----   ------------ --------
1   Job1     BackgroundJob  Completed True        localhost
3    Job3     BackgroundJob  Completed  True        localhost
5    Job5     WmiJob     Completed  True       Server-R2,loca...
9    MyRemoteJob  RemoteJob   Completed  True      Server-
R2,loca...
```

[illegible]ID[illegible]Format-List *[illegible]

```
PS C:\> get-job -id 1 | format-list *
State      : Completed
```

```
HasMoreData   : True
StatusMessage  :
Location     : localhost
Command     : dir
JobStateInfo   : Completed
Finished     : System.Threading.ManualResetEvent
InstanceId    : e1ddde9e-81e7-4b18-93c4-4c1d2a5c372c
Id       : 1
Name      : Job1
ChildJobs    : {Job2}
Output     : {}
Error      : {}
Progress     : {}
Verbose     : {}
Debug      : {}
Warning     : {}
```

[illegible] ID [illegible] Get-Job Cmdlet [illegible] ID [illegible]

[illegible] ChildJobs [illegible]

[illegible] Receive-Job [illegible] Cmdlet [illegible]

- [illegible] ID [illegible] Get-Job [illegible] Receive-Job [illegible]
- [illegible]
- [illegible] -Keep [illegible] CliXML [illegible]
- [illegible] 13 [illegible] Cmdlet [illegible] Sort-Object [illegible] Format-List [illegible] Export-CSV [illegible] ConvertTo-HTML [illegible] Out-File [illegible]

[illegible]

```
PS C:\>Receive-Job -ID 1

    Directory: C:\Users\Administrator\Documents
Mode       LastWriteTime  Length  Name
----       -------------  ------  ---------
d---- 11/21/2009 11:53 AM      Integration Services Script
Component
d---- 11/21/2009 11:53 AM      Integration Services Script Task
d----   4/23/2010 7:54 AM      SQL Server Management Studio
d----   4/23/2010 7:55 AM      Visual Studio 2005
d---- 11/21/2009 11:50 AM      Visual Studio 2008
```

[illegible]

```
PS C:\>Start-Job -ScriptBlock { Dir }
```

[illegible]PowerShell[illegible]C:\[illegible]C:\Users\Administrator\Documents[illegible]C:\[illegible]

```
PS C:\>Start-Job -ScriptBlock { Dir C:\ }
```

[illegible]Job1[illegible]-Keep[illegible]

```
PS C:\>Receive-Job -ID 1
PS C:\>
```

[illegible]

```
PS C:\>Receive-Job -ID 3 -Keep

Index Time     EntryType  Source       InstanceID  Message
----------     ----------  ---------      ----------  --------
6542 Oct 04 11:55  SuccessA...  Microsoft-Windows...     4634
An...
6541 Oct 04 11:55  SuccessA...  Microsoft-Windows...     4624
An...
6540 Oct 04 11:55  SuccessA...  Microsoft-Windows...     4672
Sp...
```

```
6539 Oct 04 11:54  SuccessA...  Microsoft-Windows...     4634
An...
```

[illegible]Cmdlet[illegible]

```
PS C:\>Receive-Job -Name MyRemoteJob | Sort-Object PSComputerName |
➥Format-Table -GroupByPSComputerName

   PSComputerName: localhost
Handles NPM(K)  PM(K)  WS(K)  VM(M)  CPU(s)  ID   ProcessName
PSComputerName
------- -----   -----   -----  -----   ------  --   -----------  --
-------------
   195     10    2780      5692     30    0.70    484 lsm
loca...
   237     38   40704  36920    547    3.17   1244 Micro...
loca...
   146     17    3260      7192     60    0.20   3492 msdtc
loca...
  1318    100   42004  28896    154   15.31   476 lsass    loca...
```

[illegible]Invoke-Command[illegible]Cmdlet[illegible]PSComputerName[illegible]

Get-Job[illegible]

```
PS C:\>Get-Job

WARNING: column "Command" does not fit into the display and was
removed.

Id     Name     State    HasMoreData   Location
--     -----    -------   ------------  --------
1     Job1     Completed  False     localhost
3     Job3     Completed  True      localhost
5     Job5     Completed  True      server-r2,lo...
8     MyRemoteJob  Completed  False     server-r2,lo...
```

[illegible]HasMoreData[illegible]False[illegible]Job1[illegible]MyRemoteJob[illegible]-Keep[illegible]

15.7 [illegible]

[illegible]

```
PS C:\>Get-Job -ID 1 | Format-List *

State      : Completed
HasMoreData   : True
StatusMessage  :
Location     :localhost
Command     :dir
JobStateInfo   : Completed
Finished     :System.Threading.ManualResetEvent
InstanceId    : e1ddde9e-81e7-4b18-93c4-4c1d2a5c372c
Id       : 1
Name      : Job1
ChildJobs     : {Job2}
Output     : {}
Error      : {}
Progress     : {}
Verbose     : {}
Debug      : {}
Warning     : {}
```

[illegible]ID[illegible]1[illegible]Start-Job –Script{Get-Service}[illegible]ID[illegible]ID[illegible]

[illegible]Job1[illegible]Job2[illegible]

```
PS C:\>Get-Job -Name Job2 | Format-List *

State     : Completed
StatusMessage  :
HasMoreData   : True
Location    :localhost
Runspace    :System.Management.Automation.RemoteRunspace
Command    :dir
JobStateInfo  : Completed
Finished    :System.Threading.ManualResetEvent
InstanceId   : a21a91e7-549b-4be6-979d-2a896683313c
Id       : 2
Name      : Job2
```

```
ChildJobs   : {}
Output     : {Integration Services Script Component, Integration
Servic
         es Script Task, SQL Server Management Studio, Visual Studi
         o 2005...}
Error     : {}
Progress    : {}
Verbose    : {}
Debug     : {}
Warning    : {}
```

[illegible]

```
PS C:\>Get-Job -ID 1 | Select-Object -Expand ChildJobs

WARNING: column "Command" does not fit into the display and was
removed.
ID     Name     State   HasMoreData   Location
---    ----     -----   -----------   ------------
2     Job2     Completed True      localhost
```

[illegible]ID[illegible]1[illegible]

[illegible]ID[illegible]Receive-Job[illegible]

15.8 [illegible]

[illegible]ID[illegible]

- Remove-Job——[illegible]
- Stop-Job——[illegible]
- Wait-Job——[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]

```
PS C:\>Get-Job | Where { -Not $_.HasMoreData } | Remove-Job
PS C:\>Get-Job

WARNING: column "Command" does not fit into the display and was
removed.

Id     Name     State   HasMoreData   Location
---    -----    ------   ------------  ------------
3     Job3     Completed True      localhost
5     Job5     Completed True      server-r2,lo...
```

[illegible]PowerShell[illegible]

```
PS C:\>Invoke-Command -Command { Nothing } -Computer NotOnline -
AsJob –Job
Name ThisWillFail

WARNING: column "Command" does not fit into the display and was
removed.

Id      Name      State  HasMoreData  Location
---     ----      -----  -----------  ------------
11      ThisWillFail  Failed  False    NotOnline
```

[illegible]State[illegible]Stop-Job[illegible]

```
PS C:\>Get-Job -ID 11 | Format-List *

State     : Failed
HasMoreData   : False
StatusMessage  :
Location    :notonline
Command    : nothing
JobStateInfo  : Failed
Finished    :System.Threading.ManualResetEvent
InstanceId   : d5f47bf7-53db-458d-8a08-07969305820e
ID       : 11
Name      :ThisWilLFail
ChildJobs   : {Job12}
Output     : {}
Error     : {}
Progress    : {}
```

```
Verbose    : {}
Debug     : {}
Warning    : {}
```

[illegible]

```
PS C:\>Get-Job -Name Job12

WARNING: column "Command" does not fit into the display and was
removed.
ID      Name      State   HasMoreData   Location
---     -----     -----   ------------  ------------
12      Job12     Failed   False     NotOnline
```

[illegible]Receive-Job[illegible]

```
PS C:\>Receive-Job -Name Job12
Receive-Job[illegible][NotOnline]Connecting to remote server failed with the
following
error message:WinRM cannot process the request. The following error
occured
while using Kerberos authentication:The network psth was not found.
```

[illegible][NotOnline][illegible]

```
PS C:\>Invoke-Command -Command { Nothing }
➥-Computer NotOnline,Server-R2 -AsJob -JobNameThisWillFail
[illegible]“Command”[illegible]
ID     Name      State   HasMoreData   Location
---    ----      ------   ------------  -----------
13     ThisWillFail  Running  True      NotOnline,Se...
```

[illegible]

```
PS C:\>Get-Job
[illegible]“Command”[illegible]
ID      Name      State  HasMoreData   Location
---     -----     ------  ------------  ------------
13      ThisWillFail  Failed  False     NotOnline,Se...
```

[illegible]

```
PS C:\>Get-Job -ID 13 | Select -Expand ChildJobs
[illegible]“Command”[illegible]
ID      Name     State  HasMoreData  Location
---     -----    ------  -----------  -----------
14      Job14    Failed  False    NotOnline
15      Job15    Failed  False    Server-R2
```

[illegible]Job14[illegible]Job15[illegible]

```
PS C:\>Receive-Job -Name Job15
Receive-Job : The term 'nothing' is not recognized as the name of a
Cmdlet, function,
script file, or operable program. Check the spelling of the name,
or if a path was
included, verify that the path is correct and try again.
```

[illegible]PowerShell[illegible]

15.9 [illegible]

[illegible]v3[illegible]PowerShell[illegible]——[illegible]Windows[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]New-JobTrigger[illegible]New-ScheduledTaskOption[illegible]Register-ScheduledJob[illegible]XML[illegible]

[illegible]

```
PS C:\> Register-ScheduledJob -Name DailyProcList -ScriptBlock {
Get-Process }
-Trigger (New-JobTrigger -Daily -At 2am) –ScheduledJobOption
(New-ScheduledJobOption -WakeToRun -RunElevated)
```

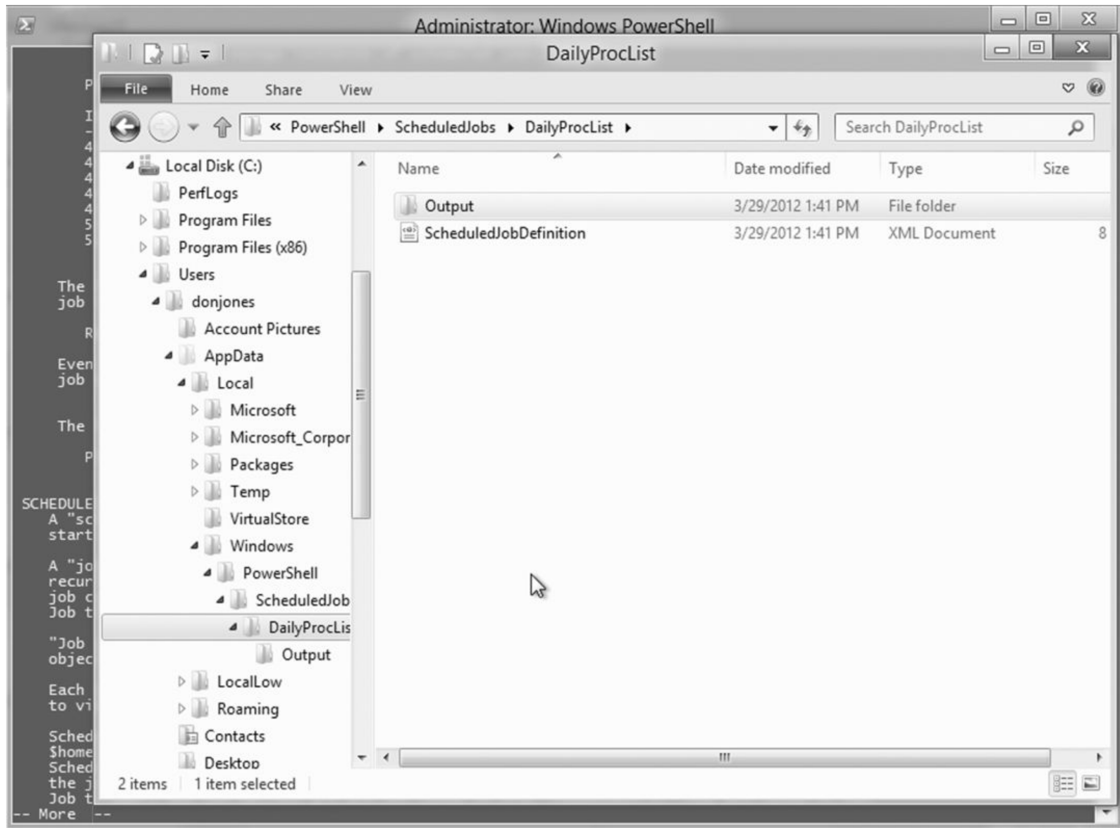
```
□□: □“Enabled”□□□□□□□□□□
ID      Name       JobTriggers    Command
---     ----       -----------    --------------
1      DailyProcList  {1}      Get-Process
```

□□□□□□□□□□□□□□□□□□□□□□□Get-Process□□PowerShell□□□□Get-Job□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\>Get-Job
□□: □“Command”□□□□□□□□□□
ID     Name       State     HasMoreData    Location
---    --------    -------    ------------   ------------
6     DailyProcList  Completed  True       localhost
9     DailyProcList  Completed  True       localhost
```

□□□15.1□□□□□□□□□□□□□□□□□□□□□□□□□□Receive-Job□□□□□□□□□□□□

□□□□□Register-ScheduledJob□□□-MaxResultCount□□□□□□□□□□□□□□□



□15.1 □□□□□□□□□□□□□□□

15.10 □□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\>Invoke-Command -Command { Start-Job -ScriptBlock { Dir } }
➥-ComputerName Server-R2
```

□□□□□□□□□□Server-R2□□

□□□□□□□□□□□□□□□□□□□□

```
PS C:\>Start-Job -ScriptBlock { Invoke-Command -Command { Dir }
➥-ComputerName SERVER-R2 }
```

□□□□□□□□□□□□□□□□Invoke-Command□□□□□□□-AsJob□□□□□
□□□□□□□□□

□□□“□
□□□□□□□□□□□□□□□□□□”□□□□□□“□□”□□□□□□□□□□□□□□□□□□□
PowerShell□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Office Word□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□Word□□□□□

□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□
□□□
□□□□□□□□□□□□□□□

15.11 □□□□

□□□□□□□□□□□□□□□□□□□□□□□□□Windows 8□□□□□□□
Windows Server 2012□□□□□□□PowerShell□□□□□

□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□
□□□

1□□□□□□□□□□□□□□C:□□□□□□PowerShell□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□

2□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□
□□□□□1□□□□□□□□

3□□□□□□□□□□□□□□□□□□□□□□□□□□25□□□□□□□□□□□□□□
CliXML□□□□□□□□□□□□6□□□□□□□□□□□□□□□□□□□

4□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□16□　□□□□□□□□

PowerShell□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□3□□□□□□□□□□□□□□□□□□□□
□□□Cmdlet□WMI□□□□□□□□□

16.1　□□□□□□□□□□

□□□□□□□□□□□□□□VBScript□□□□□□□□□□□□VBScript□□□□□□□□□□□
□□□□——Don□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□
□□□□□□□

```
For Each varService in colServices
   varService.ChangeStartMode("Automatic")
Next
```

□□□□□□□□□VBScript□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□1□□□□□colServices□□□□□□□□□□colServices□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□

□2□For Each□□□□□□□□□□□□□□□□□□□□□□□□□□□□□varService□□□
□□□□varService□□□□□□□□□□□□colServices□□50□□□□□□□□□□□□□□□
50□□□□□varService□□□□□□□□50□□□□□□□□

□3□□□□□□□□□□□□□□□□□——□□□□□ChangeStartMode()□□——□□
□□□□□

□□□
□□□□□GUI□□

□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□VBScript□□□□□□□□□□□

PowerShell□□
□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□PowerShell□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□

16.2 □□□□□“□□□”Cmdlet

　　□□□□□□□□□□□□PowerShell Cmdlet □□□□□□□□□□□□□□□□□□

　　□□□6□□□□□□□□□□□□□Cmdlet□□□□□□□□□Cmdlet□□□□□□□
□□□□□□□□——□□□□□□□□□□

```
Get-Service | Stop-Service
```

　　□□□□□□□□□□□□□□□□□Stop-Service□□□□□□□□□□□□□□□□□
□□□□□□□Set-Service□Stop-Service□Move-ADObject□□Move-Mailbox□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□
VBScript□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□
□□

　　□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□3□□□□□□□□□□□□VBScript□□□□□□□□□□□□□

```
Get-Service -name BITS,Spooler,W32Time | Set-Service -startuptype
Automatic
```

　　□□□□□□□Get-Service□□□□□□Cmdlet□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□

```
Get-Service -name BITS,Spooler,W32Time -computer
Server1,Server2,Server3 |
Set-Service -startuptype Automatic
```

　　□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□-passThru□□□□□□□□
□□□□□□□□□□□□□□□Set-Service□□□□□□□□□□Get-Service□□□□
□□□□□□□□□□□□□□□

　　□□□□Cmdlet□□-PassThru□□□□□

```
Get-Service -name BITS -computer Server1,Server2,Server3 |
Start-Service -passthru |
Out-File NewServiceStatus.txt
```

□□□□□3□□□□□□□□□□□□□□□□□□□□□□□Start-Service□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Out-File□□□□□□□□□□□□□□□□□

□□□□□□□□□□PowerShell□□□□□□□□□□□□□Cmdlet□□□□□□□Cmdlet□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□

16.3 MI□□□□□WMI□□

□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□Windows□□□□WMI□□□□□□□□□□□□WMI□□□□□□14□□□□

□□□ □□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□

□□WMI□Win32_NetworkAdapterConfiguration□□□intel□□□□DHCP□□□□□□□RAS□□□□□□DHCP□

□□□□□□□□□□□□□□□□□□□

```
DHCPEnabled       : False
IPAddress         : {192.168.10.10, fe80::ec31:bd61:d42b:66f}
DefaultIPGateway :
DNSDomain    :
ServiceName     : E1G60
Description    : Intel(R) PRO/1000 MT Network Connection
Index      : 7

DHCPEnabled    : True
IPAddress    :
DefaultIPGateway :
DNSDomain    :
ServiceName    : E1G60
Description    : Intel(R) PRO/1000 MT Network Connection
Index      : 12
```

□□□□□□□□□□□□□□□□WMI□□□□□□□□□□INTEL□□□□□□□□□□□□□□□□WMI□□□“%”□□□□□□

```
PS C:\> gwmi win32_networkadapterconfiguration
➥-filter "description like '%intel%'"
```

Intel

DHCP

DHCP “Enable-DHCP” Cmdlet

Cmdlet Cmdlet Cmdlet WMI

DHCP Get-Member Gm

```
PS C:\> gwmi win32_networkadapterconfiguration
➡ -filter "description like '%intel%'" | gm
```

EnableDHCP

```
TypeName: System.Management.ManagementObject#root\cimv2\Win32_NetworkAd
apterConfiguration

Name                          MemberType    Definition
----                          ----------    ----------
DisableIPSec               Method
System.Management.ManagementB...
EnableDHCP                    Method
System.Management.ManagementB...
EnableIPSec                   Method
System.Management.ManagementB...
EnableStatic                  Method
System.Management.ManagementB...
```

PowerShell

```
PS C:\> gwmi win32_networkadapterconfiguration
➡ -filter "description like '%intel%'" | EnableDHCP()
```

Cmdlet

EnableDHCP PowerShell Cmdlet

VBScript VBScript

PowerShell

Enable-DHCP “ ” Cmdlet Invoke-WmiMethod Cmdlet Cmdlet WMI

Win32 _NetworkAdapter Confiuration

```
PS C:\> gwmi win32_networkadapterconfiguration
➥ -filter "description like '%intel%'" |
➥ Invoke -WmiMethod -name EnableDHCP
```

[illegible]

- [illegible]
- [illegible]
- Invoke-WmiMethod[illegible]WMI[illegible]Win32_NetworkAdapterConfiguration[illegible]
- [illegible]Invoke-WmiMethod[illegible]-WhatIf[illegible]-Conifrm[illegible]

Invoke-WmiMethod[illegible]WMI[illegible]

```
__GENUS           : 2
__CLASS            : __PARAMETERS
__SUPERCLASS      :
__DYNASTY          : __PARAMETERS
__RELPATH          :
__PROPERTY_COUNT  : 1
__DERIVATION     : {}
__SERVER          :
__NAMESPACE       :
__PATH             :
ReturnValue      : 0

__GENUS            : 2
__CLASS            : __PARAMETERS
__SUPERCLASS      :
__DYNASTY          : __PARAMETERS
__RELPATH          :
__PROPERTY_COUNT  : 1
__DERIVATION      : {}
__SERVER           :
__NAMESPACE       :
__PATH             :
ReturnValue       : 84
```

[illegible]ReturnValue[illegible]Google[illegible]“Win32_NetworkAdapterConfiguration”[illegible]EnableDHCP[illegible]16.1[illegible]

0[illegible]84[illegible]IP[illegible]DHCP[illegible]WMI[illegible]

79	Invalid security parameter.
80	Unable to configure TCP/IP service.
81	Unable to configure DHCP service.
82	Unable to renew DHCP lease.
83	Unable to release DHCP lease.
84	IP not enabled on adapter.
85	IPX not enabled on adapter.
86	Frame or network number bounds error.
87	Invalid frame type.
88	Invalid network number.

[illegible]16.1 [illegible]WMI[illegible]

[illegible]WMI[illegible]Invoke-WmiMethod[illegible]“[illegible]Get-WmiObject[illegible]Invoke-WmiObject[illegible]”[illegible]

[illegible]14[illegible]Get-WmiObject[illegible]Invoke-WmiMethod[illegible]“[illegible]”[illegible]WMI[illegible]Cmdlet[illegible]Get-CimInstanc[illegible]Invoke-CimMethod[illegible]

```
PS C:\> Get-CimInstance -classname win32_networkadapterconfiguration
➥ -filter "description like '%intel%'" |
➥ Invoke-CimMethod -methodname EnableDHCP
```

[illegible]14[illegible]WMI[illegible]CIM[illegible]WMI[illegible]RPC[illegible]WMI[illegible]CIM[illegible]WS-MAN[illegible]Windows[illegible]WS-MAN[illegible]

[illegible]WMI[illegible]14[illegible]WMI[illegible]Cmdlet[illegible]WMI[illegible]PowerShell[illegible]Help Set-NetIPAddress[illegible]Windows[illegible]Cmdlet[illegible]WMI[illegible]Cmdlet[illegible]IP[illegible]WMI[illegible]PowerShell[illegible]PowerShell v1[illegible]v2[illegible]v3[illegible]Cmdlet[illegible]4[illegible]5[illegible]

16.4 [illegible]

[illegible]Invoke-WmiObject[illegible]——[illegible]Cmdlet[illegible]Cmdlet[illegible]VBScript[illegible]PowerShell[illegible]Cmdlet[illegible]21[illegible]21[illegible]PowerShell[illegible]

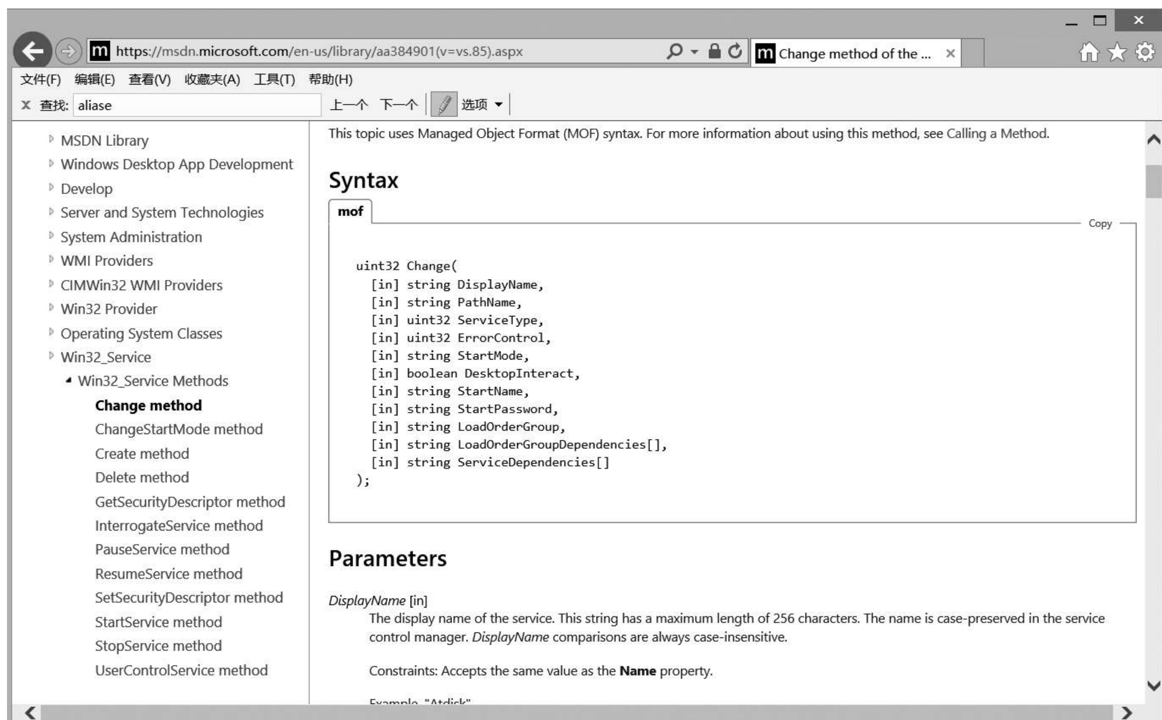
[illegible]Win32_Service[illegible]WMI[illegible]Change()[illegible]16.2[illegible]“Win32_Service”[illegible]Change[illegible]

[illegible]Null[illegible]PowerShell[illegible]$null[illegible]

[illegible]8[illegible]7[illegible]$null[illegible]

```
Change($null, $null, $null, $null, $null, $null, $null, "P@ssw0rd")
```

[illegible]Get-Service[illegible]Set-Service[illegible]WMI[illegible]WMI[illegible]



□16.2 in32_Service□Change()□□□□□□

□□□□□□□□□□□□Set-Service□□□□□Cmdlet□□□□□□□□□□□□□□□□□□Invoke-WmiMethod□□Cmdlet□□□□□□□-ArgumentList□□□

```
PS C:\> gwmi win32_service -filter "name = 'BITS'" | invoke-wmimethod -name
 change -arg $null,$null,$null,$null,$null,$null,$null,"P@ssw0rd"
Invoke-WmiMethod : Input string was not in a correct format.
At line:1 char:62
+ gwmi win32_service -filter "name = 'BITS'" | invoke-wmimethod <<<<  -nam
e change -arg $null,$null,$null,$null,$null,$null,$null,"P@ssw0rd"
    + CategoryInfo          : NotSpecified: (:) [Invoke-WmiMethod], Forma
   tException
    + FullyQualifiedErrorId : System.FormatException,Microsoft.PowerShell
   .Commands.InvokeWmiMethod
```

□□□ □□□□□□□□Get-WmiObject□□Get-CimInstance□□□□□□□□□□

□□Invoke-WmiMethod□Chang()□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

[illegible]

[illegible]Shell[illegible]Change()[illegible]ForEach-Object[illegible]Cmdlet[illegible]

```
PS C:\> gwmi win32_service -filter "name = 'BITS'" | foreach-object
{$_.cha
nge($null,$null,$null,$null,$null,$null,$null,"P@ssw0rd") }

__GENUS            : 2
__CLASS            : __PARAMETERS
__SUPERCLASS      :
__DYNASTY          : __PARAMETERS
__RELPATH          :
__PROPERTY_COUNT  : 1
__DERIVATION      : {}
__SERVER           :
__NAMESPACE       :
__PATH             :
ReturnValue       : 0
```

[illegible]ReturnValue[illegible]0[illegible]

```
Get-WmiObject Win32_Service -filter "name = 'BITS'" |
➥ ForEach-Object -process {
➥  $_.change($null,$null,$null,$null,$null,$null,$null,"P@ssw0rd")
➥ }
```

[illegible]Get-WmiObject[illegible]Win32_Service[illegible]“BITS”[illegible]BITS[illegible]Win32_Service[illegible]ForEach-Object[illegible]Cmdlet[illegible]

[illegible]

- [illegible]Cmdlet[illegible]ForEach-Object[illegible]
- [illegible]-Process[illegible]-Process[illegible]-Process[illegible]
- ForEach-Object[illegible]ForEach-Object[illegible]$_[illegible]
- [illegible]$_[illegible]“.”[illegible]Shell[illegible]

- □□□□□□□□□Change()□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$null□□□□□□□□□□□□□□□□□□□□□□□8□□□□□□□□□□□□□□□□□□□□□□□□□□□9□□□10□□□11□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$null□□

  □□□□□□□□□□□□□□□□16.3□□□□□□□□

Get-WmiObject Win32_Service -filter "name = 'BITS'" |
ForEach-Object -process { $_.Change($null,$null,$null,$null,$null,$null,$null,"P@ssw0rd") }

命令名称
参数名称
方法名称
忽略的几个方法参数
我们希望指定的方法参数
对象容器以及作用域

□16.3 □□ForEach-Object Cmdlet

□□□□WMI□□□□□□□□□□□□□□□□□□□□Invoke-WmiMethod□□ForEach-Object□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□

```
PS C:\> gwmi win32_service -fi "name = 'BITS'" |
➥ % {$_.change($null,$null,$null,$null,$null,$null,$null,"P@ssw0rd") }
```

□□□□□□□□□□□□□□□

- □□□□Gwmi□□□Get-WmiObject□
- □□□-filter□□□-fi□
- □□□□%□□□□□□ForEach-Object□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□-Process□□□□□□□□□□□□□□□□□□□

□□□Tab□□□□□□□Shell□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□16.4□□

WMI类
过滤条件
Get-WmiObject Win32_Service -filter "name = 'BITS'" |
ForEach-Object -process { $_.Change($null,$null,$null,$null,$null,$null,$null,"P@ssw0rd") }
方法名称
参数列表，只会出现在圆括号内

- [illegible]WMI[illegible]WMI[illegible]
- [illegible]Change[illegible]
- [illegible]“argument”[illegible]EnableDHCP()[illegible]

[illegible]Set-Service[illegible]Get-Wmi-Object[illegible]Get-CimInstance[illegible]PowerShell v3[illegible]WMI[illegible]

16.5 [illegible]

[illegible]PowerShell[illegible]

16.5.1 [illegible]

[illegible]“[illegible]Cmdlet”[illegible]“[illegible]Cmdlet”[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]“[illegible]”[illegible]

[illegible]Cmdlet[illegible]100%[illegible]Cmdlet[illegible]Cmdlet[illegible]PowerShell[illegible]

```
Get-Service -name *B* | Stop-Service

Get-Service -name *B* | ForEach-Object { $_.Stop() }

Get-WmiObject Win32_Service -filter "name LIKE '%B%' |
➥Invoke-WmiMethod -name StopService

Get-WmiObject Win32_Service -filter "name LIKE '%B%' |
➥ForEach-Object { $_.StopService() }

Stop-Service -name *B*
```


[illegible]

- [illegible]Cmdlet❶[illegible]Get-Service[illegible]“B”[illegible]
- [illegible]ForEach-Object[illegible]Cmdlet[illegible]Stop()[illegible]❷[illegible]
- [illegible]WMI[illegible]Shell[illegible]Cmdlet❸[illegible]“B”[illegible]Invoke-WmiMethod[illegible]StopService[illegible]WMI[illegible]
- [illegible]ForEach-Object[illegible]Invoke-WmiMethod[illegible]❹[illegible]2[illegible]3[illegible]
- [illegible]Stop-Service❺[illegible]-Name[illegible]PowerShell v3[illegible]

[illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]Cmdlet[illegible]WMI[illegible]

- [illegible]Cmdlet[illegible]“*”[illegible]WMI[illegible]%[illegible]——[illegible]ForEach-Object[illegible]Get-WmiObject[illegible]-filter[illegible]
- [illegible]WMI[illegible]Get-Service[illegible]ServiceController[illegible]Stop()[illegible]WMI[illegible]Win32_Service[illegible]StopService()[illegible]
- [illegible]-eq[illegible]WMI[illegible]=[illegible]Like[illegible]

[illegible]?[illegible]“[illegible]”[illegible]Shell[illegible]

16.5.2 WMI[illegible]Cmdlet[illegible]

[illegible]WMI[illegible]Cmdlet[illegible]?[illegible]

- [illegible]Get-WmiObject[illegible]WMI[illegible]Invoke-WmiMethod[illegible]ForEach-Object[illegible]
- [illegible]Get-WmiObject[illegible]Cmdlet[illegible]Cmdlet[illegible]ForEach-Object[illegible]

[illegible]ForEach-Object[illegible]

[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]ForEach-Object[illegible]

[illegible]Get-Something[illegible]Cmdlet[illegible]Delete-Something[illegible]Remove-Something[illegible]Cmdlet[illegible]Delete[illegible]

```
Get-Something | ForEach-Object { $_.Delete() }
```

16.5.3 [illegible]

[illegible]Get-Member[illegible]Get-Something[illegible]Cmdlet[illegible]

```
Get-Something | Get-Member
```

PowerShell[illegible]WMI[illegible]WMI[illegible]WMI[illegible]PowerShell[illegible]WMI[illegible]Stop[illegible]Start[illegible]

```
TypeName: System.ServiceProcess.ServiceController

Name            MemberType    Definition
----            ----------    ----------
Name            AliasProperty  Name = ServiceName
RequiredServices       AliasProperty  RequiredServices =
ServicesDepe...
Disposed           Event      System.EventHandler Disposed(Sy...
Close            Method     System.Void Close()
Continue           Method     System.Void Continue()
CreateObjRef         Method     System.Runtime.Remoting.ObjRef ...
Dispose           Method     System.Void Dispose()
Equals           Method     bool Equals(System.Object obj)
ExecuteCommand        Method     System.Void ExecuteCommand(int ...
GetHashCode         Method     int GetHashCode()
GetLifetimeService      Method     System.Object GetLifetimeService()
GetType           Method     type GetType()
InitializeLifetimeService   Method     System.Object
InitializeLifetim...
Pause            Method     System.Void Pause()
```

```
Refresh          Method     System.Void Refresh()
Start            Method     System.Void Start(), System.Voi...
Stop             Method     System.Void Stop()
ToString         Method     string ToString()
WaitForStatus    Method     System.Void WaitForStatus(Syste...
```

[illegible]TypeName[illegible]System.Service Process.ServiceController[illegible]

16.5.4 ForEach-Object[illegible]

ForEach-Object[illegible]Cmdlet[illegible]

- [illegible]ForEach-Object[illegible]%[illegible]ForEach[illegible]
- [illegible]
- [illegible]$_[illegible]
- [illegible]$_[illegible]$_[illegible]“.”[illegible]
- [illegible]

16.6 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]

1[illegible]ServiceController[illegible]Get-Service[illegible]

2[illegible]Process[illegible]Get-Process[illegible]

3[illegible]WMI[illegible]Win32_Process[illegible]

4[illegible]4[illegible]“Notepad”[illegible]

[illegible]17[illegible] [illegible]

[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]PowerShell[illegible]

17.1 [illegible]Shell[illegible]

[illegible]2006[illegible]PowerShell[illegible]VBScript[illegible]Windows Script Host(WSH)[illegible]“I Love You”“Melissa”[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]

[illegible]PowerShell[illegible]•[illegible]“[illegible]”[illegible]“[illegible]”[illegible]PowerShell[illegible]“[illegible]”[illegible](Writing secure code)[illegible]PowerShell[illegible] ——[illegible]

17.2 Windows PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]

[illegible]

[illegible]SAPIEM PrimalScript(www.PrimalTools.com)[illegible]

[illegible](.EXE)[illegible]PowerShell[illegible]

[illegible]

PowerShell[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]

17.3 [illegible]

PowerShell[illegible]PowerShell[illegible]

17.3.1 [illegible]

[illegible]Restricted[illegible]PowerShell[illegible]PowerShell[illegible]

```
□□□□□□ C:\test.ps1□□□□□□□□□□□□□□□□□□□□□□□□ "get
-help about_signing"□
□□□□□:1 □□: 11
+ .\test.ps1 <<<<
    + CategoryInfo          : NotSpecified: (:) [], PSSecurityException
    + FullyQualifiedErrorId :RuntimeException
```

□□□□□□□Get-ExecutionPolicy□□□

- □□Set-ExecutionPolicy□□□□□□□□□□Windows□□□□□HKEY_LOCAL_MACHINE□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□GPO□□□Windows Server 2008 R2□□□Windows PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ADM□□□□□□□□□□□□□□□□□□□□□□□http://mng.bz/U6tJ □□□□□□□□□□□□□□□□□□□□http://download.microsoft.com□□□□□□□□□□PowerShell ADM□□□□□

□□17.1□□□□□□□□“□□□□□□□”>□□□□>□□□□>Windows□□>Windows PowerShell□□□PowerShell□□□□□□17.2□□□□□□□□□□□“□□”□□□Set-ExecutionPolicy□□□



□17.1 Windows PowerShell□□□□□□□□□



□17.2 □□□□□□□□□Windows PowerShell□□□□□

- □□□□□□PowerShell.exe□□□□□-ExecutionPolicy□□□

  □□□□□□□□□□□5□□□□□□□□□□□□□□□□□□□□□3□□□□□

- Restricted——□□□□□□□□□□□□□□□□□□PowerShell□□
- AllSigned——□□□□□□□□□□□□□CA□□□□□□□□□□□□□□□□□□PowerShell□□□□□
- RemoteSigned——PowerShell□□□□□□□□□□□□□□□□□□□CA□□□□□□□□□□□□□□□□□□□□□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□UNC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□□□”□Internet

Explorer[illegible] Firefox[illegible]Outlook[illegible]
[illegible]Windows[illegible]UNC[illegible]UNC[illegible]
[illegible]“[illegible]”[illegible]

- Unrestricted——[illegible]
  [illegible]
- Bypass——[illegible]PowerShell[illegible]
  [illegible]

[illegible]

[illegible]PowerShell.exe[illegible]
[illegible]GPO[illegible]

[illegible]

[illegible]PowerShell[illegible]
PowerShell[illegible].Net[illegible]

[illegible]RemoteSigned[illegible]Restricted[illegible]RemoteSigned[illegible]AllSigned[illegible]
PowerShell[illegible]

[illegible]

> **[illegible]** [illegible]Unrestricted[illegible]

17.3.2 [illegible]

[illegible]

```
<!-- SIG # Begin signature block -->
<!-- MIIXXAYJKoZIhvcNAQcCoIIXTTCCF0kCAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB -
->
<!-- gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR -
->
```

```
<!-- AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQUJ7qroHx47PI1dIt4lBg6Y5Jo -->
<!-- UViggHIxMIIEYDCCA0ygAwIBAgIKLqsR3FD/XJ3LwDAJBgUrDgMCHQUAMHAxKzAp -->
<!-- YjcCn4FqI4n2XGOPsFq7OddgjFWEGjP1O5igggyiX4uzLLehpcur2iC2vzAZhSAU -->
<!-- DSq8UvRB4F4w45IoaYfBcOLzp6vOgEJydg4wggR6MIIDYqADAgECAgphBieBAAAA -->
<!-- ZngnZui2t++Fuc3uqv0SpAtZIikvz0DZVgQbdrVtZG1KVNvd8d6/n4PHgN9/TAI3 -->
<!-- an/xvmG4PNGSdjy8Dcbb5otiSjgByprAttPPf2EKUQrFPzREgZabAatwMKJbeRS4 -->
<!-- kd6Qy+RwkCn1UWIeaChbs0LJhix0jm38/pLCCOo1nL79E1sxJumCe6GtqjdWOIBn -->
<!-- KKe66D/GX7eGrfCVg2Vzgp4gG7fHADFEh3OcIvoILWc= -->
<!-- SIG # End signature block -->
```


[illegible] PowerShell [illegible]

[illegible] CA [illegible] Cybertrust [illegible] GoDaddy [illegible] Thawte [illegible] VeriSign [illegible] PKI [illegible] CA [illegible] —— [illegible] XYZ [illegible] CA [illegible] XYZ [illegible] CA [illegible] CA [illegible] CA [illegible]

[illegible] Windows [illegible] IE [illegible] Content [illegible] Publishers [illegible] “[illegible]” [illegible] 17.3 [illegible] CA [illegible]

证书

预期目的(N): <所有>

个人 | 其他人 | 中间证书颁发机构 | 受信任的根证书颁发机构 | 受信任的发布者 | 未受信任的发布者

颁发给	颁发者	截止日...	友好名称
ABC	ABC	2023-...	<无>
ABC TEST CA	ABC TEST CA	2023-...	<无>
ABC2048	ABC2048	2033-...	<无>
AddTrust External CA ...	AddTrust Exte...	2020-...	USERTrust
Alibaba.com Corporati...	Alibaba.com C...	2016-...	<无>
ALIPAY_ROOT	ALIPAY_ROOT	2018-...	<无>
Baltimore CyberTrust ...	Baltimore Cyb...	2025-...	Baltimore ...
CareySon.cloudapp.net	CareySon.clou...	2023-...	<无>
CareySon-PC	CareySon-PC	3012-...	<无>
CareySon-PC	CareySon-PC	2024-...	VisualSVN ...

导入(I)... 导出(E)... 删除(R) 高级(A)

证书的预期目的

<所有>

查看(V)

关闭(C)

[illegible]17.3 [illegible]“[illegible]”[illegible]

[illegible]CA[illegible]CA[illegible]——[illegible]“[illegible]”[illegible]CA[illegible]CA[illegible]CA[illegible]

[illegible]——[illegible]CA[illegible]PowerShell[illegible]Set-AuthenticodeSignatureCmdlet[illegible]PowerShell[illegible]Help About_Signing[illegible]PrimalScript[illegible]PowerShell Plus[illegible]PowerGUI[illegible]

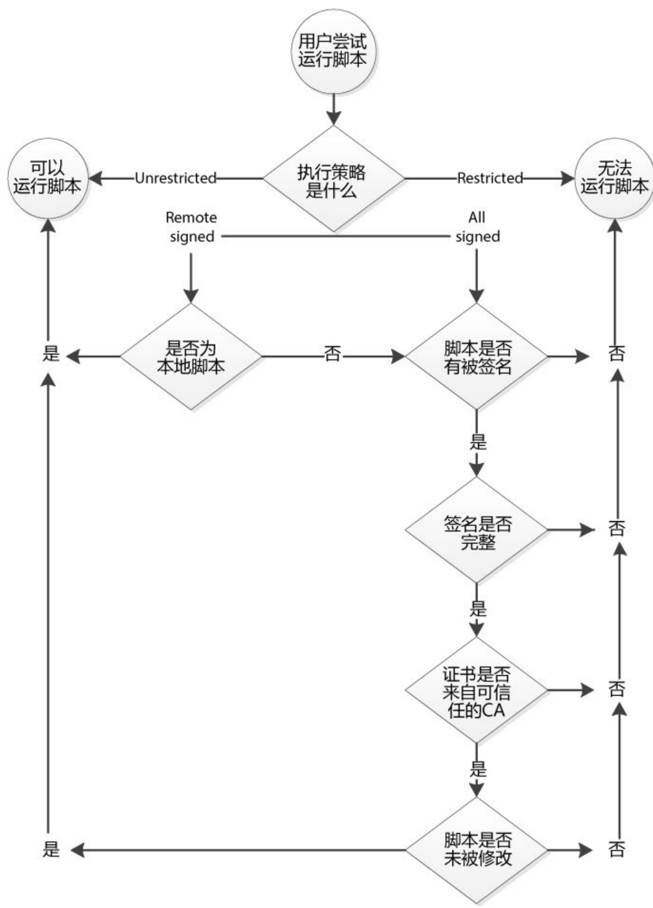
[illegible]

[illegible]1[illegible]

[illegible]2[illegible]

[illegible]3[illegible]PowerShell[illegible]

[illegible]17.4[illegible]PowerShell[illegible]AllSigned[illegible]



[illegible]17.4 [illegible]PowerShell[illegible]

17.4 [illegible]

PowerShell[illegible]

[illegible]Windows[illegible]PS1[illegible]PowerShell[illegible]PS1[illegible]PowerShell[illegible]PS1[illegible]PowerShell[illegible]

[illegible]Shell[illegible]Shell[illegible]test.PS1[illegible]test[illegible]test.PS1[illegible]

[illegible]

```
PS C:\> test
[illegible]“test”[illegible]Cmdlet[illegible]
[illegible]:1 [illegible]:5
+ test<<<<
     + CategoryInfo          : ObjectNotFound: (test:String) [],
CommandNo
   tFoundException
     + FullyQualifiedErrorId :CommandNotFoundException

Suggestion [3,General]: [illegible] test[illegible]Windows PowerSh
ell [illegible] ".\test"[illegible]
[illegible] "get-help about_Command_Precedence"[illegible]
PS C:\>
```

[illegible]PowerShell[illegible]test.PS1[illegible]C:[illegible]C:\test[illegible].\test[illegible]

[illegible]“[illegible]”[illegible]Dir[illegible]PowerShell[illegible]——[illegible]Dir[illegible].\Dir[illegible]Dir.PS1[illegible]

17.5 [illegible]

[illegible]PowerShell[illegible]Shell[illegible]Shell[illegible]PowerShell[illegible]——[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

Program Files Delete
PowerShell

PowerShell

17.6

PowerShell
RemoteSigned AllSigned Unrestricted

AllSigned

- CA 900 PKI Help About_Signing MakeCert.exe
-

.PS1 Windows .PS1 VBScript

MoreLunches.com

17.7

PowerShell v3 PowerShell

—— MoreLunches.com PowerShell Set-ExecutionPolicyCmdlet RemoteSigned

AllSigned[illegible]
Unrestricted[illegible]

[illegible]PowerShell[illegible]

[illegible]18[illegible] [illegible]

[illegible]PowerShell[illegible]“[illegible]”[illegible]

18.1 [illegible]

[illegible]“[illegible]”[illegible]“[illegible]”[illegible]XML[illegible]

PowerShell[illegible]

18.2 [illegible]

PowerShell[illegible]——[illegible]Get-Member[illegible]Gm[illegible]“System.String”[illegible]

```
PS C:\> "SERVER-R2" | gm

   TypeName: System.String

Name           MemberType        Definition
----           ----------         ----------
Clone          Method              System.Object Clone()
CompareTo      Method              int CompareTo(System.Object
valu...
Contains       Method              bool Contains(string value)
CopyTo          Method              System.Void CopyTo(int
sourceInd...
EndsWith        Method             bool EndsWith(string value),
boo...
Equals          Method              bool Equals(System.Object obj),
```

```
...
GetEnumerator   Method              System.CharEnumerator
GetEnumera...
GetHashCode    Method              int GetHashCode()
GetType         Method              type GetType()
GetTypeCode    Method              System.TypeCode GetTypeCode()
IndexOf         Method               int IndexOf(char value), int
Ind...
IndexOfAny      Method               int IndexOfAny(char[] anyOf),
in...
```

[illegible]“System.String”[illegible]

[illegible]Shell[illegible]“SERVER-R2”[illegible]VM[illegible]PM[illegible]Name[illegible]CPU[illegible]ID[illegible]

PowerShell[illegible]=[illegible]

```
PS C:\> $var = "SERVER-R2"
```

[illegible]“SERVER-R2”[illegible]

[illegible]$[illegible]“var”[illegible]“$”[illegible]Shell[illegible]

- [illegible]
- [illegible]
- [illegible]${My Variable}[illegible]“My Variable”[illegible]
- [illegible]Shell[illegible]Shell[illegible]
- [illegible]——[illegible]“computername”[illegible]“processes”[illegible]
- [illegible]VBScript[illegible]PowerShell[illegible]VBScript[illegible]“strComputerName”[illegible]

□“str”□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□

□□
Shell□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□

```
PS C:\> $var
SERVER-R2
```

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□
□□□

```
PS C:\> get-wmiobject win32_computersystem -comp SERVER-R2

Domain               : company.pri
Manufacturer        : VMware, Inc.
Model                : VMware Virtual Platform
Name                : SERVER-R2
PrimaryOwnerName     : Windows User
TotalPhysicalMemory : 3220758528
```

□□□□□□□□□□□□□□□□□□

```
PS C:\> get-wmiobject win32_computersystem -comp $var

Domain               : company.pri
Manufacturer        : VMware, Inc.
Model                : VMware Virtual Platform
Name                 : SERVER-R2
PrimaryOwnerName    : Windows User
TotalPhysicalMemory : 3220758528
```

□□□□□var□□□□□□□□□□□□□□□□□□□□□□“computername”□□□□□□□□□□
□□□□□□□□□□□□□□□□□□$var□□□□□□□□□□□□□□□□□□□□var□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□

□□□□□□□□$var□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $var = 5
PS C:\> $var | gm
   TypeName: System.Int32
```

```
Name          MemberType  Definition
----           ---------- ----------
CompareTo    Method     int CompareTo(System.Object value), int
CompareT...
Equals       Method      bool Equals(System.Object obj), bool
Equals(int ...
GetHashCode  Method       int GetHashCode()
GetType      Method       type GetType()
GetTypeCode  Method       System.TypeCode GetTypeCode()
ToString    Method       string ToString(), string ToString(string
format...
```

□□□□□□□□□□□□□□□□□□$var□□□□$var□Gm□□□□□□□□□□□□□Shell□$var□□□□□□System.Int32□□□□32□□□□

18.3 □□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $var = 'What does $var contain?'
PS C:\> $var
What does $var contain?
```

□□□□□□□□□□□□□□□□□□□□□□□□$var□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $computername = 'SERVER-R2'
PS C:\> $phrase = "The computer name is $computername"
PS C:\> $phrase
The computer name is SERVER-R2
```

□□□□□“SERVER-R2”□□□□"$computername"□□□□□□$phrase□□□“"The computer name is $computername"”□□□□□□□□□□□□PowerShell□□□$phrase□□□□□□$computername□□□“SERVER-R2”□□□

□□□□□□□□□□□Shell□□□□□□□□□□□□□□□$phrase□□□□“The computer name is SERVER-R2”——□□□□□□“$computername”□□□

□□□□□□□□$computername□□□□□$phrase□□□□□□□

```
PS C:\> $computername = 'SERVER1'
PS C:\> $phrase
The computer name is SERVER-R2
```

□□□□□$phrase□□□□□□□□□□□

□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□`□□□□□□□□□□□□□□□□□Esc□□□□□□□□□□□~□□Consolas□□□□□□□Lucida Console □Raster□□□□□□□□□□□

□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□18.1 □□□Consolas □□□□□□□OK□□□□□□□□□□□□□□□□□□□□□□□□□□□18.1 □□



[illegible]

```
PS C:\> $computername = 'SERVER-R2'
PS C:\> $phrase = "`$computername contains $computername"
PS C:\> $phrase
$computername contains SERVER-R2
```

[illegible]$phrase[illegible]$computername[illegible]$computername[illegible]$computername[illegible]

[illegible]

```
PS C:\> $phrase = "`$computername`ncontains`n$computername"
PS C:\> $phrase
$computername
contains
SERVER-R2
```

[illegible]`n——[illegible]$computername[illegible]contains[illegible]“n”[illegible]n[illegible]new line[illegible]

[illegible]“help about_escape”[illegible]“t”[illegible]tab[illegible]“a”[illegible]a[illegible]alert[illegible]

18.4 [illegible]

[illegible]

[illegible]PowerShell[illegible]

```
PS C:\> $computers = 'SERVER-R2','SERVER1','localhost'
PS C:\> $computers
SERVER-R2
```

```
SERVER1
Localhost
```

[illegible] PowerShell [illegible]

18.4.1 [illegible]

[illegible] 0 [illegible] 1 [illegible] 1 [illegible] 2 [illegible]

```
PS C:\> $computers[0]
SERVER-R2
PS C:\> $computers[1]
SERVER1
PS C:\> $computers[-1]
localhost
PS C:\> $computers[-2]
SERVER1
```

[illegible]

```
PS C:\> $computers.count
3
```

[illegible]

```
PS C:\> $computername.length
9
PS C:\> $computername.toupper()
SERVER-R2
PS C:\> $computername.tolower()
server-r2
PS C:\> $computername.replace('R2','2008')
SERVER-2008
PS C:\> $computername
SERVER-R2
```

[illegible]$computername[illegible]System.String[illegible]18.2 [illegible]Gm[illegible]Length[illegible]ToUpper()[illegible]ToLower()[illegible]Replace()[illegible]ToUpper()[illegible]ToLower()[illegible]——[illegible]

18.4.2 [illegible]

[illegible]$computers[illegible]PowerShell v2[illegible]

```
PS C:\> $computers.toupper()
Method invocation failed because [System.Object[]] doesn't contain a
metho
d named 'toupper'.
At line:1 char:19
+ $computers.toupper <<<< ()
    + CategoryInfo          : InvalidOperation: (toupper:String) [],
Runt
   imeException
    + FullyQualifiedErrorId : MethodNotFound
```

[illegible]

```
PS C:\> $computers[0].tolower()
server-r2
PS C:\> $computers[1].replace('SERVER','CLIENT')
CLIENT1
```

[illegible]

```
PS C:\> $computers
SERVER-R2
SERVER1
Localhost
```

[illegible]

```
PS C:\> $computers[1] = $computers[1].replace('SERVER','CLIENT')
PS C:\> $computers
SERVER-R2
CLIENT1
Localhost
```

[illegible]PowerShell v2[illegible]v3[illegible]

18.4.3 [illegible]

[illegible]ToLower()[illegible]

```
PS C:\> $computers = $computers | ForEach-Object { $_.ToLower() }
PS C:\> $computers
server-r2
client1
localhost
```

[illegible]18.2[illegible]$computers =[illegible]

[illegible]$computers[illegible]“ForEach-Object”[illegible]Cmdlet[illegible]3[illegible]$_[illegible]ToLower()[illegible]ToLower()[illegible]——[illegible]$computers[illegible]

[illegible]“Select-Object”[illegible]Length[illegible]

```
PS C:\> $computers | select-object length

Length

------

9

7

```

```
9
```

□□□□□□□□□□□PowerShell□□□□□□□□□□□□□

管道连接的结果将被
存储在这个变量中
PS C:\> $computers = $computers | ForEach-Object { $_.ToLower() }
把这个变量的内
容放入管道中
枚举命令
中的对象
对每一个对象
执行这个方法

□18.2 □□“ForEach-Object”□□□□□□□□□□□□□□□□

18.4.4 □PowerShell□□□□□□□□

“□□□□□□□□□□□□□□□□□□□□□□”□□□□□□PowerShell v1□v2 □□□□□□□□□□□□□□□v3□□□□□□□□□□□□□□□□□“automatic unrolling”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
$services = Get-Service
$services.Name
```

□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□$services□□□□□□□□□□□□□——□□□

```
Get-Service | ForEach-Object { Write-Output $_.Name }
```

□□□□□□

```
Get-Service | Select-Object –ExpandProperty Name
```

□□□□□□□v1 □v2□□□□□□□□□□□□□□□□□□

```
$objects = Get-WmiObject –class Win32_Service –filter "name='BITS'"
$objects.ChangeStartMode('Disabled')
```

□□□□□□PowerShell v3□□□□□□□□□——□□□□□□□□□□□□□□□□□

18.5 [illegible]

[illegible] $service[illegible]

```
PS C:\> $services = get-service
PS C:\> $firstname = "$services[0].name"
PS C:\> $firstname
AeLookupSvc ALG AllUserInstallAgent AppIDSvc Appinfo AppMgmt
AudioEndpoint
Builder Audiosrv AxInstSV BDESVC BFE BITS BrokerInfrastructure
Browser bth
serv CertPropSvc COMSysApp CryptSvc CscService DcomLaunch defragsvc
Device
AssociationService DeviceInstall Dhcp Dnscache dot3svc DPS DsmSvc
Eaphost
EFS ehRecvr ehSched EventLog EventSystem Fax fdPHost FDResPub fhsvc
FontCa
che gpsvc hidserv hkmsvc HomeGroupListener HomeGroupProvider IKEEXT
iphlps
vc KeyIso KtmRm LanmanServer LanmanWorkstation lltdsvc lmhosts LSM
Mcx2Svc
 MMCSS MpsSvc MSDTC MSiSCSI msiserver napagent NcaSvc NcdAutoSetup
Netlogo
n Netman netprofm NetTcpPortSharing NlaSvc nsi p2pimsvc p2psvc
Parallels C
oherence Service Parallels Tools Service PcaSvc PeerDistSvc PerfHost
pla P
lugPlay PNRPAutoReg PNRPsvc PolicyAgent Power PrintNotify ProfSvc
QWAVE Ra
sAuto RasMan RemoteAccess RemoteRegistry RpcEptMapper RpcLocator
RpcSs Sam
Ss SCardSvr Schedule SCPolicySvc SDRSVC seclogon SENS SensrSvc
SessionEnv
SharedAccess ShellHWDetection SNMPTRAP Spooler sppsvc SSDPSRV
SstpSvc stis
vc StorSvc svsvc swprv SysMain SystemEventsBroker TabletInputService
TapiS
rv TermService Themes THREADORDER TimeBroker TrkWks TrustedInstaller
UI0De
tect UmRdpService upnphost VaultSvc vds vmicheartbeat
vmickvpexchange vmic
rdv vmicshutdown vmictimesync vmicvss VSS W32Time wbengine WbioSrvc
Wcmsvc
 wcncsvc WcsPlugInService WdiServiceHost WdiSystemHost WdNisSvc
WebClient
Wecsvc wercplsupport WerSvc WiaRpc WinDefend WinHttpAutoProxySvc
```

```
Winmgmt W
inRM WlanSvc wlidsvc wmiApSrv WMPNetworkSvc WPCSvc WPDBusEnum wscsvc
WSear
ch WSService wuauserv wudfsvc WwanSvc[0].name
```

[illegible]$services[illegible]“[”[illegible]PowerShell[illegible]$services[illegible][0].name[illegible]

[illegible]

```
PS C:\> $services = get-service
PS C:\> $firstname = "The first name is $($services[0].name)"
PS C:\> $firstname
The first name is AeLookupSvc
```

[illegible]$()[illegible]PowerShell[illegible]$()[illegible]

[illegible]PowerShell v3[illegible]PowerShell v3[illegible]Shell[illegible]$service[illegible]

```
PS C:\> $services = get-service
PS C:\> $var = "Service names are $services.name"
PS C:\> $var
Service names are AeLookupSvc ALG AllUserInstallAgent AppIDSvc
Appinfo App
Mgmt AudioEndpointBuilder Audiosrv AxInstSV BDESVC BFE BITS
BrokerInfrastr
ucture Browser bthserv CertPropSvc COMSysApp CryptSvc CscService
DcomLaunc
h defragsvc DeviceAssociationService DeviceInstall Dhcp Dnscache
dot3svc D
PS DsmSvc Eaphost EFS ehRecvr ehSched EventLog EventSystem Fax
fdPHost FDR
esPub fhsvc FontCache FontCache3.0.0.0 gpsvc hidserv hkmsvc
HomeGroupListe
ner HomeGroupProvider IKEEXT iphlpsvc KeyIso KtmRm LanmanServer
LanmanWork
station lltdsvc lmhosts LSM Mcx2Svc MMCSS MpsSvc MSDTC MSiSCSI
msiserver M
SSQL$SQLEXPRESS napagent NcaSvc NcdAutoSetup Netlogon Netman
netprofm NetT
```

```
cpPortSharing NlaSvc nsi p2pimsvc p2psvc Parallels Coherence Service
Paral
lels Tools Service PcaSvc PeerDistSvc PerfHost pla PlugPlay
PNRPAutoReg PN
RPsvc PolicyAgent Power PrintNotify ProfSvc QWAVE RasAuto RasMan
RemoteAcc
ess RemoteRegistry RpcEptMapper RpcLocator RpcSs SamSs SCardSvr
Schedule S
CPolicySvc SDRSVC seclogon SENS SensrSvc SessionEnv SharedAccess
ShellHWDe
```

[illegible]

18.6 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

[illegible]

```
PS C:\> $number = Read-Host "Enter a number"
Enter a number: 100
PS C:\> $number = $number * 10
PS C:\> $number
100100100100100100100100100100
```

[illegible]“Read-Host”——[illegible]——[illegible]

[illegible]100[illegible]10[illegible]100100100100100100100100100100[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]100[illegible]10[illegible]100[illegible]10[illegible]100[illegible]10[illegible]

[illegible]

```
PS C:\> $number = Read-Host "Enter a number"
Enter a number: 100
PS C:\> $number | gm

   TypeName: System.String

Name           MemberType        Definition
----              ----------        ----------
Clone          Method             System.Object Clone()
CompareTo        Method             int CompareTo(System.Object
valu...
Contains         Method              bool Contains(string value)
```

□□□$number□□□□□Gm□□□□□Shell□□□System.String□□□System.Int32□□□□□□□□□□□□□□□□□□□□□□□

□□□□Shell□□$number□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□□□□□□□[]□□□□□□□□□“int”□□□□

```
PS C:\> [int]$number = Read-Host "Enter a number"
Enter a number: 100
PS C:\> $number | gm

   TypeName: System.Int32

Name        MemberType Definition
----        ---------- ----------
CompareTo   Method     int CompareTo(System.Object value), int CompareT...
Equals      Method     bool Equals(System.Object obj), bool Equals(int ...
GetHashCode Method     int GetHashCode()
GetType     Method     type GetType()
GetTypeCode Method     System.TypeCode GetTypeCode()
ToString    Method     string ToString(), string ToString(string format...

PS C:\> $number = $number * 10
PS C:\> $number
1000
```


□□□□□□□□□□[int]□□$number□□□□❶□□□□□□□□□$number□□□□□Gm□□□□□□□□□□□□□□❷□□□□□□□□□□□□□□□□□□□□□□□□□❸□

□□□□□□□□□□□Shell□□□□□□□□□□□□Shell□□□□□□□$number□□□□□□□□□□

```
PS C:\> [int]$number = Read-Host "Enter a number"
Enter a number: Hello
Cannot convert value "Hello" to type "System.Int32". Error: "Input
```

```
string
was not in a correct format."
At line:1 char:13
+ [int]$number <<<<  = Read-Host "Enter a number"
    + CategoryInfo          : MetadataError: (:) [],
ArgumentTransformati
   onMetadataException
    + FullyQualifiedErrorId : RuntimeException
```

□□□□□□□□□□□□□□□□□□□$number□□□□□□□□

□□[int]□□□□□□□□□□□□□□□□□□□□□□□□□

- [int]——□□□□□
- [single]□[double]——□□□□□□□□□□□□□□□□□□□□□
- [string]——□□□□
- [char]——□□□□□□[char]$c='X'□□
- [xml]——□□XML□□□□□□□□□□□□□□□□□□□□□□□XML□□□□□ [xml]$doc=Get-Content MyXML.xml□□
- [adsi]——□□□□□□□□□□ADSI□□□□Shell□□□□□□□□□□□□□□□ [adsi]$user="WinNT:\MYDOMAIN\Administrator,user"□□

□□□ □□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> [int]$x = 5
PS C:\> $x = 'Hello'
Cannot convert value "Hello" to type "System.Int32". Error: "Input string
was not in a correct format."
At line:1 char:3
+ $x <<<<  = 'Hello'
    + CategoryInfo          : MetadataError: (:) [], ArgumentTransformati
   onMetadataException
    + FullyQualifiedErrorId : RuntimeException

PS C:\> [string]$x = 'Hello'
PS C:\> $x | gm

   TypeName: System.String

Name             MemberType          Definition
----             ----------          ----------
Clone            Method              System.Object Clone()
CompareTo        Method              int CompareTo(System.Object valu...
```

❶ 定义变量$x 为整型

❷ 创建一个错误,并把错误信息放到$x 中

❸ 以字符形式重新对$x 赋值

❹ 确认$x 的新类型

□□□□□□□□□□□□□□□□□□$x□□□□□❶□□□□□□□□□□□□□□□□□□ □□□□□□□□❷□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

[illegible]❸[illegible]Gm[illegible]❹[illegible]

18.7 [illegible]

[illegible]PowerShell[illegible]Option Explicit[illegible]VBScript[illegible]PowerShell[illegible]Set-StrictMode[illegible]Shell[illegible]

- New-Variable[illegible]
- Set-Variable[illegible]
- Remove-Variable[illegible]
- Get-Variable[illegible]
- Clear-Variable[illegible]

[illegible]“Remove-Variable”[illegible]Del[illegible]——[illegible]——[illegible]ad hoc syntax[illegible]Cmdlets[illegible]

[illegible]Cmdlets[illegible]Cmdlets[illegible]-name [illegible]——[illegible]out-of-scope[illegible]Cmdlets[illegible]“help about_scope”[illegible]

18.8 [illegible]

[illegible]

- [illegible]$computername[illegible]$c[illegible]$computer_to_query_for_data [illegible]
- [illegible]
- [illegible]PrimalScript[illegible]

18.9 常见误区

当涉及数据存储的时候，许多人在变量的使用上经常会犯一些错误，比如变量名称中使用的特殊字符、双引号中变量的替换等。但Shell总有一些功能可以帮助我们避免这些错误。我们来看一下这些功能。

Shell提供的功能主要有以下两个方面：

- 如果能确保变量名称只包含字母、数字或下划线，那么就可以很容易地避免使用大括号。而且这也使得使用变量名称时可以使用Tab键进行补全。
- 在本章中我们讲解了如何使用数组来存储多个值。而在使用数组时，需要注意如何访问数组中的单个元素。

18.10 动手实验

> 注意： 对于本次动手实验，你需要运行PowerShell v3或更高版本PowerShell的计算机。

请按第15章所学内容，或者查看相关帮助文件完成以下练习任务：

1．创建一个后台作业，从两台计算机上查询Win32_BIOS类的信息。如果你只有一台计算机，可以将计算机名称“localhost”输入两次。

2．当后台作业完成时，将作业结果放入一个变量中。

3．显示该变量的内容。

4．将该变量的内容导出到CliXML格式文件。

18.11 进一步学习

请花几分钟，浏览一下前面几章的内容，然后尝试思考一下哪些命令结果可以放入变量中，以方便以后使用。

比如，在第13章中，你学过了如何使用远程处理。你可以在远程处理中使用变量吗？比如，如果需要对多台计算机执行命令，是否可以先将计算机名称放入变量中？在第20章中，你将会学习到更多关于变量的知识。

[illegible]19[illegible] [illegible]

[illegible]PowerShell[illegible]
[illegible]
[illegible]

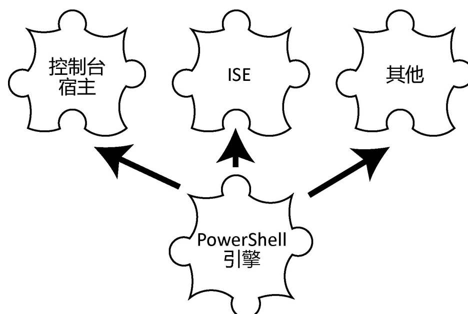
19.1 [illegible]

PowerShell[illegible]PowerShell[illegible]
[illegible]PowerShell[illegible]

[illegible]PowerShell.exe[illegible]
[illegible]PowerShell ISE[illegible]ISE[illegible]
[illegible]PowerShell[illegible]
[illegible]

[illegible]19.1[illegible]PowerShell[illegible]
[illegible]
PowerShell[illegible]ISE[illegible]
[illegible]ISE[illegible]
[illegible]“OK”[illegible]

[illegible]
[illegible]ISE[illegible]Shell[illegible]PowerShell
[illegible]



□19.1 □□□□□□□□□□PowerShell□□

19.2 Read-Host□□

PowerShell□Read-Host Cmdlet□□□Cmdlet□□□□□□□□□□□□

```
PS C:\> Read-Host "Enter a computer name"
Enter a computer name: SERVER-R2
SERVER-R2
```

□□□□□Cmdlet□□□□□□□□

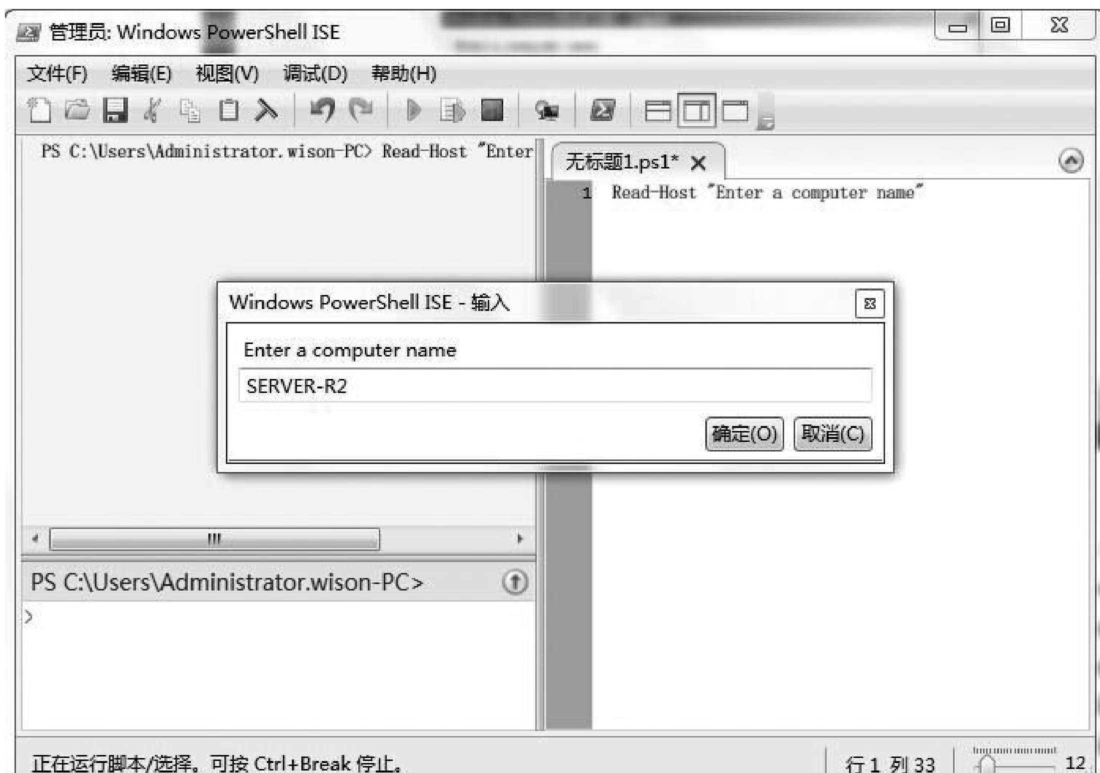
- □□□□□□□□□□□□□
- □□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $ComputerName=Read-Host "Enter a computer name"
Enter a computer name: SERVER-R2
```

□□□□□□□□□□□□□□□□□□□□$ComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□Server-2□□□□□□□Server-2□

□□□□□□□□□□PowerShell ISE□□□□□□□□□□□□□□□□□□□□□□19.2□□□□□□□□□□□□□PowerGUI□PowerShell Plus□□PrimalScript□□□□□□□□□□□□□□□□□□Read-Host□□□□□□□□PowerShell ISE□□□□□□□□□□□□□□□□PowerShell ISE□□□□□□PowerShell ISE□□□□□□□□□□□□□□□□□□□□□



□19.2 □□□□ISE□□Read-Host□□□□□□□□□

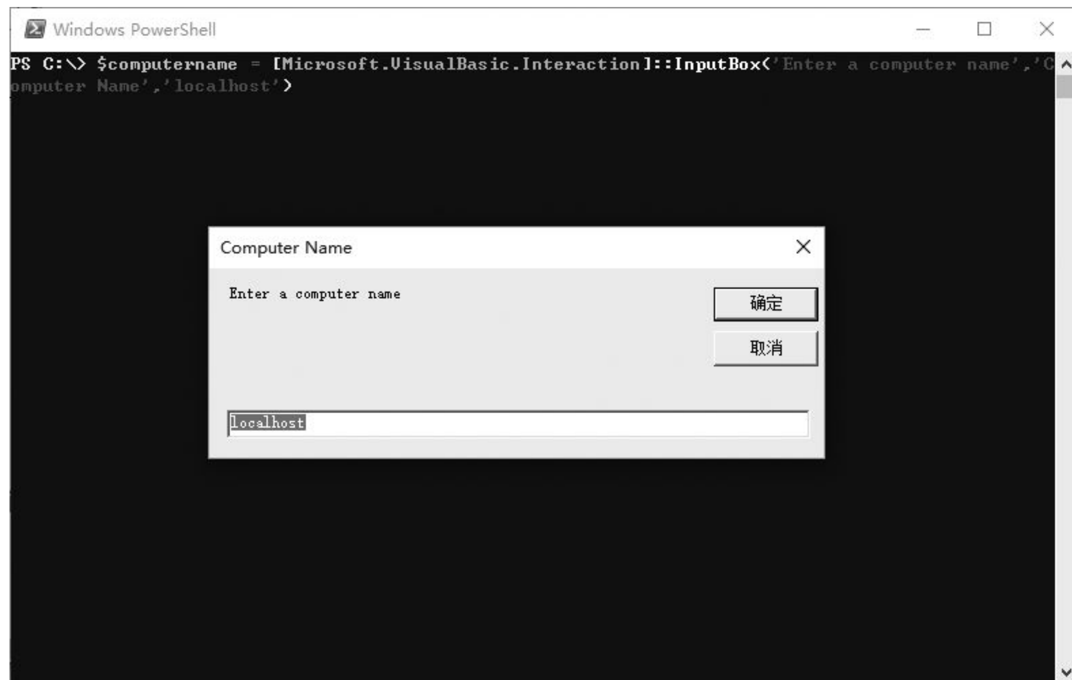
□□Read-Host□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□Read-Host□□□□□□□□□□□□□□□"□□□□□□□□□□□□□□□□□□□□□□□□□"□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"Windows□□"□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□19.3□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□.Net Framework□□□□□□□□□□□□□

```
PS C:\> [void]
[System.Reflection.Assembly]::LoadWithPartialName('Microsoft.
➥VisualBasic')
```

□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□.Net Framework□□□□□□Microsoft.VisualBasic□□□□PowerShell□□□□□□□□□□□□□□Framework□□□□□□□□VisualBasic□□□□□□□□□□□□□□□□□□□□□□□□



[illegible]19.3 [illegible]Windows PowerShell[illegible]

[illegible]

- [Void][illegible][Void][illegible]Void[illegible]“[illegible]”[illegible]Void[illegible]Out-Null[illegible]
- [illegible]System.Reflection.Assembly[illegible]PowerShell[illegible]
- [illegible]LoadWithPartialName()[illegible]Framework[illegible]

[illegible]Framework[illegible]

```
PS C:\> $ComputerName =
[Microsoft.VisualBasic.Interaction]::InputBox('Enter a
➥computer name','Computer Name','localhost')
```

[illegible]Microsoft.VisualBasic.InterAction[illegible]“[illegible]”[illegible]——[illegible]

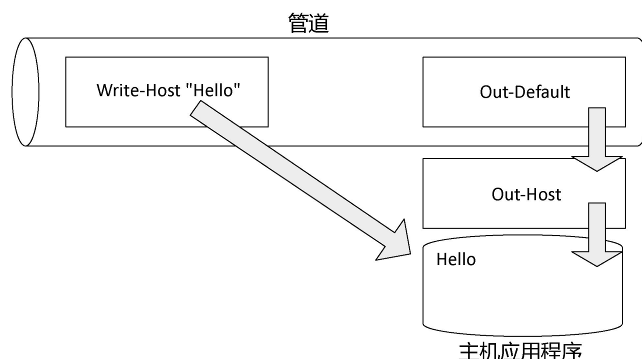
[illegible]InputBox()[illegible]

- [illegible]
- [illegible]
- [illegible]——[illegible]

[illegible]Read-Host[illegible]

19.3 Write-Host[illegible]

[illegible]Write-Host[illegible]



[illegible]19.4 Write-Host[illegible]

[illegible]19.4[illegible]Write-Host[illegible]Cmdlet[illegible]-ForegroundColor[illegible]-BackgroundColor[illegible]

```
PS C:\> Write-Host "COLORFUL!" -Fore Yellow -Back Magenta
COLORFUL!
```

[illegible]

[illegible] [illegible]PowerShell[illegible]

[illegible]Write-Host[illegible]

[illegible]Write-Host[illegible]——[illegible]PowerShell[illegible]_Learn PowerShell Toolmaking in a Month of Lunches (Manning, 2012)_[illegible]Write-Host[illegible]——[illegible]PowerShell[illegible]Write-Host[illegible]

[illegible] [illegible]Write-Host[illegible]“[illegible]”[illegible]——[illegible]“nowconnec ting to Server-2”[illegible]“testing for folder”[illegible]Write-Verbose[illegible]

[illegible]

[illegible]22[illegible]Write-Verbose[illegible]Write Cmdlet[illegible]Write-Verbose[illegible]

[illegible]Write Cmdlet[illegible]$VerbosePreference= "Continue"[illegible]Write-Verbose[illegible]$VerbosePreference="SilentlyCon tinue"[illegible]Write-Debug[illegible]$DebugPreference[illegible]Write-Warning[illegible]$WarningPreference[illegible]“Preference”[illegible]

[illegible]22[illegible]Write-Verbose[illegible]

[illegible]Write-Host[illegible]Cmdlet[illegible]Write-Verbose[illegible]PowerShell[illegible]

19.4 Write-Output□□

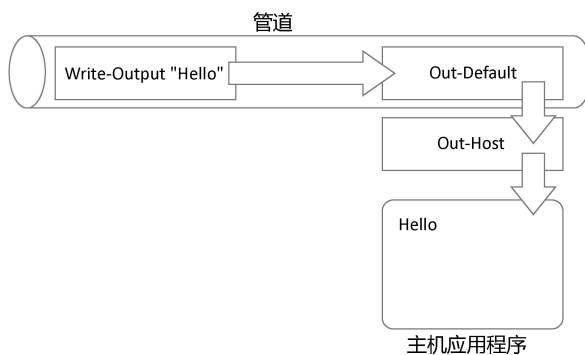
□□Write-Host□□□Write-Output□□Write-Output□□□□□□□Write□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□□19.5□□□□□□□□□□□

□□□□□□□10□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□1□Write-Output□□□String□□□□□Hello□□□□□□□

□2□□□□□□□□□□□□□□Hello□□□□□□□□□□□□□Out-Default□□□□□□

□3□Out-Default□□□□□□□□Out-Host□□□



□19.5 Write-Output□□□□□□□□□□□□□□□□□□□□□□□□□□□

□4□Out-Host□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□String□□□□□□□□□□□□□□String□□□□□□□□

□5□Out-Host□□□□□□□□□□□□□□□□

□□□□□□□□□Write-Host□□

```
PS C:\> Write-Output "Hello" | Where-Object { $_.Length -GT 10 }
```

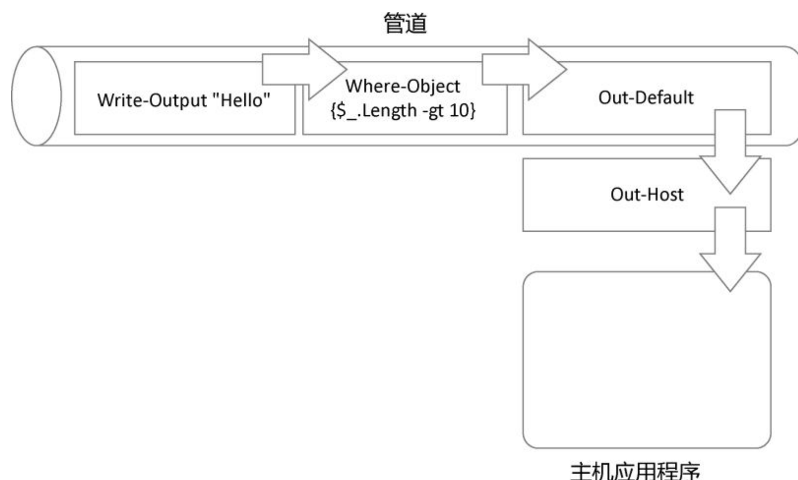
[illegible]19.6[illegible]“Hello”[illegible]Out-Default[illegible]Where-Object[illegible]Length[illegible]10[illegible]“Hello”[illegible]Out-Default[illegible]Out-Host[illegible]

[illegible]

```
PS C:\> Write-Host "Hello" | Where-Object { $_.Length -GT 10 }
Hello
```

[illegible]Write-Host[illegible]Write-Output[illegible]“Hello”[illegible]Where-Object[illegible]Out-Default[illegible]Out-Host[illegible]“Hello”[illegible]

Write-Output[illegible]PowerShell[illegible]Cmdlet[illegible]PowerShell[illegible]PowerShell[illegible]Write-Output[illegible]



[illegible]19.6 [illegible]

19.5 [illegible]

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□Write-Host□□□□□□□□□□□□□□□□□□□□Write-Host□□□□□□□□□□□□□□□□□□□□□□□□□

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“Continue”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“SilentlyContinue”□□□□□□□□□□□□□□□□□□□□□□□19.1□□□□□Cmdlet□□□□

□19.1 □□□□□Cmdlet

Cmdlet	□□	□□□□
Write-Warning	□□□□□□□□□□□□□□□□□□□□□□□□“□□□”□□	$WarningPreference □□□□Continue□
Write-Verbose	□□□□□□□□□□□□□□□□□□□□□□□□“□□□□□”□□	$VerbosePreference □□□□SilentlyContinue□
Write-Debug	□□□□□□□□□□□□□□□□□□□□□□□“□□□”□□	$DebugPreference (□□□SilentlyContinue)
Write-Error	□□□□□□□□	$ErrorActionPreference (□□□Continue)

Write-Error□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□

□□□PowerShell□□□□□Cmdlet Write-Progress□□Cmdlet□□

□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□“Continue”□□□□□□□□□□□□Cmdlet□□□□□□□□□□□SilentlyContinue□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□

□□□ □PowerShell□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□PrimalScript□□PowerShell□□□□□□Cmdlet□□□□□□

19.6 □□□□

Write-Host和Write-Output之间的区别是什么？我们有一个简单的练习来帮助你理解。你可以从MoreLunches.com找到这个练习的答案。

1．使用Write-Output显示数字100和10的乘积。

2．使用Write-Host显示数字100和10的乘积。

3．提示用户输入名字，然后使用红色文本显示名字。

4．提示用户输入一个数字，然后显示除以5的结果。这个结果用黄色文本显示——使用适当的命令。

如果你想要更多练习的话，可以尝试对本章中的Cmdlet进行实验。请记住，我们在本书其他章节中已经讲过了很多关于输出的内容——在交互方面，那些章节也同样值得参考。

在本章中，我们讨论了与用户进行交互的不同方法，参见本书第3章。

19.7 进一步学习

我们建议你花一些时间学习本章所讲的Cmdlet，以及其他以写入为主的Cmdlet。在接下来的章节中，我们会使用这些内容。你可以尝试对本章中的Cmdlet进行实验，在进一步学习之前，确保你已经掌握了这些内容。

□20□ □□□□□□□□

□□13□□□□□□□□PowerShell□□□□□□□□□□13□□□□□□□□□□□□□□□□□□Cmdlet——Invoke-Command□Enter-PSSession——□□

□□

20.1 PoweShell□□□□□□□□□□

□□□□Invoke-Command□Enter-PSSession□□□

□□

20.2 □□□□□□□□□□

□□□□□□□□PowerShell□□□□□PowerShell□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Shell□

□□□□□New-PSSesion□□Cmdlet□□PowerShell□□□□□□□□□

```
PS C:\> new-pssession -computername server-r2,server17,dc5
```

Get-PSSession

```
PS C:\> get-pssession
```

Session Don IIS Web Invode-Command

```
PS C:\> $iis_servers = new-pssession -comp web1,web2,web3
➥ -credential WebAdmin
```

Shell Shell

Remove-PSSession Cmdlet IIS

```
PS C:\> $iis_servers | remove-pssession
```

```
PS C:\> get-pssession | remove-pssession
```

$sessions localhost Server-R2 Localhost PowerShell PowerShell 13

localhost

[illegible]

```
$s_server1,$s_server2 = new-pssession -computer server-r2,dc01
```

[illegible]Server-R2[illegible]$s_server1[illegible]DC01[illegible]$s_server2[illegible]

[illegible]$s_server1[illegible]DC01[illegible]Server-R2[illegible]

[illegible]

```
PS C:\> $sessions = New-PSSession -comp SERVER-R2,localhost
```

[illegible]13[illegible]

20.3 [illegible]Enter-PSSession[illegible]

[illegible]13[illegible]Enter-PSSession[illegible]Shell[illegible]$session[illegible]18[illegible]

```
PS C:\> enter-pssession -session $sessions[0]
[server-r2]: PS C:\Users\Administrator\Documents>
```

[illegible]Exit-PSSession[illegible]

```
[server-r2]: PS C:\Users\Administrator\Documents>exit-pssession
psc:\>
```

[illegible]$sessions[illegible]Gm[illegible]

```
PS C:\> $sessions | gm

   TypeName: System.Management.Automation.Runspaces.PSSession

Name                  MemberType    Definition
------                   ------------    ----------
Equals                  Method        bool Equals(System.Object
obj)
GetHashCode            Method         int GetHashCode()
GetType                Method        type GetType()
ToString               Method        string ToString()
ApplicationPrivateData  Property
System.Management.Automation.PSPr...
Availability             Property
System.Management.Automation.Runs...
ComputerName          Property      System.String ComputerName
{get;}
ConfigurationName      Property       System.String
ConfigurationName {...
Id                     Property       System.Int32 Id {get;}
InstanceId             Property       System.Guid InstanceId
{get;}
Name                  Property       System.String Name {get;set;}
Runspace               Property
System.Management.Automation.Runs...
State                   ScriptProperty  System.Object State
{get=$this.Ru...
```

[illegible]ComputerName[illegible]

```
PS C:\> enter-pssession -session ($sessions |
➥where { $_.computername -eq 'server-r2' })
[server-r2]: PS C:\Users\Administrator\Documents>
```

[illegible]

[illegible]PowerShell[illegible]Get-PSSession[illegible]

```
PS C:\> enter-pssession -session (get-pssession -computer server-
r2)
```

Get-PSSession[illegible]Server-R2[illegible]Enter-PSSession[illegible]-Session[illegible]

[illegible]Enter-PSSession[illegible]-Session[illegible]

```
-Session <PSSession>
    Specifies a Windows PowerShell session (PSSession) to use for
the
    interactive session. This parameter takes a session object.
You can
    also use the Name, InstanceID, or ID parameters to specify a
    PSSession.

    Enter a variable that contains a session object or a command
that

    creates or gets a session object, such as a New-PSSession or
Get-
    PSSession command. You can also pipe a session object to
Enter-
    PSSession. You can submit only one PSSession with this
parameter. If
    you enter a variable that contains more than one PSSession,
the
    command fails.
    When you use Exit-PSSession or the EXIT keyword, the
interactive
    session ends, but the PSSession that you created remains open
and a

    vailable for use.
    Required?                false
    Position?                1
    Default value
    Accept pipeline input?    true (ByValue, ByPropertyName)
Accept wildcard characters? True
```

[illegible]9[illegible]-Session[illegible]PSSession[illegible]Get-PSSession[illegible]PSSession[illegible]

```
PS C:\> Get-PSSession -ComputerName SERVER-R2 | Enter-PSSession
[server-r2]: PS C:\Users\Administrator\Documents>
```

[illegible]

[illegible] [illegible]PowerShell[illegible]

20.4 [illegible]Invoke-Command[illegible]

Invoke-Command[illegible]Session[illegible]$Session[illegible]

```
PS C:\> invoke-command -command { get-wmiobject -class
win32_process }
➥ -session $sessions
```

[illegible]Get-WmiObject[illegible]Get-WmiObject[illegible]-computername[illegible]4[illegible]

- [illegible]WMI[illegible]Windows[illegible]WMI[illegible]WMI[illegible]
- [illegible]Invoke-Command[illegible]Cmdlet[illegible]
- [illegible]32[illegible]WMI[illegible]
- [illegible]Get-WmiObject[illegible]Invoke-Command[illegible]

[illegible] [illegible]PowerShell v3[illegible]CIM Cmdlet[illegible]Get-CimInstance[illegible]Get-WmiObject[illegible]-computerName[illegible]Cmdlet[illegible]Invoke-Command[illegible]

Invoke-Command[illegible]-Session[illegible]“loc”[illegible]

```
PS C:\> invoke-command -command { get-wmiobject -class
win32_process }
```

```
➥ -session (get-pssession -comp loc*)
```

□□□□□□Invoke-Command□□□□□□□□□□□□□□□□Enter-PSSession□□□□□□□□□□Invoke-Command□□

20.5 □□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□PowerShell□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□□Windows Server 2008 R2□□□□□□□□□□□□□ActiveDirectory□□□□□□□□□□□□□□□□□□□□□□□□Windows Server 2008 R2□□□□□□□□□□□□□□□□□□Remote Server Administration Tools□RSAT□□Windows 7□□□□□□□□□□□□□□□□□Windows XP□Windows Vista□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $session = new-pssession -comp server-r2
PS C:\> invoke-command -command
➥{ import-module activedirectory }
➥-session $session
PS C:\> import-pssession -session $session
➥-module activedirectory
➥-prefix rem

ModuleType Name                      ExportedCommands
---------- ----                      ----------------
Script     tmp_2b9451dc-b973-495d... {Set-ADOrganizationalUnit, Get-ADD...
```

① Establishes connection 建立连接

② 载入远程控制模块

③ 导入远程控制命令

④ 查看临时本地模块

□□□□□□□□□□□□□□

① □□□PowerShell v2□□□□□□□□□Windows Server 2008 R2□□□

② [illegible]PSSnapin[illegible]

③ [illegible]“rem”[illegible]Shell[illegible]

④ PowerShell[illegible]PowerShell[illegible]

[illegible]New-remADUser[illegible]New-ADUser[illegible]“rem”[illegible]Shell[illegible]Shell[illegible]

[illegible]

[illegible]——[illegible]PowerShell[illegible]

[illegible]XML[illegible]PowerShell[illegible]

20.6 [illegible]

PowerShell v3[illegible]

[illegible]Enter-PSSession[illegible]-

ComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Admin1□□Domain Admins□□□□□□□□□□□□□Computer1□□□□□□□□□□□□□□□□□Computer2□□□□

```
PS C:\> New-PSSession -ComputerName COMPUTER2

Id  Name               ComputerName  State
--  -----------------  -------------  -----
 4  Session4            COMPUTER2     Opened
```

□□□□□□□□□□□□□□□□□Computer1□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Computer2□□□□□PowerShell□□□□□□□□□□□□□□Session□ID□□□□□□□□ID□□□□□□□□□Session□□□□

```
PS C:\> Disconnect-PSSession -Id 4

Id  Name               ComputerName   State
--  ------------------ -------------  -----
 4  Session4           COMPUTER2     Disconnected
```

□□□□□□□□□□□□——□□Computer2□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□Session□□

□□□□□□□□□□□□□□□□□□□□□□□□□Computer3□□□□□□□□□Admin1□□□□□□□Computer2□□□□□□□

```
PS C:\> Get-PSSession -computerName COMPUTER2

Id  Name                ComputerName   State
--  ------------------ -------------- -----
 4  Session4            COMPUTER2      Disconnected
```

□□□Computer2□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> Get-PSSession -computerName COMPUTER2 | Connect-PSSession

Id  Name             ComputerName  State
--  ---------------- ------------- -------
 4  Session4          COMPUTER2     Open
```

[illegible]PowerShell[illegible]WSMAN[illegible]Drive[illegible]

[illegible]

[illegible]WSMan:\localhost\Shell[illegible]:

- -IdleTimeout[illegible]Shell[illegible] Shell [illegible] Shell [illegible]2 000[illegible]84[illegible]
- -MaxConcurrentUsers[illegible] Shell [illegible]
- -MaxShellRunTime[illegible] IdleTimeout[illegible]
- -MaxShellsPerUser[illegible] Shell [illegible]MaxConcurrentUsers [illegible]

[illegible]WSMan:\localhost\Service[illegible]:

- -MaxConnections [illegible]Shell[illegible]MaxConnections[illegible]

[illegible]Shell[illegible]

20.7 [illegible]

> **[illegible]** [illegible]PowerShell v3[illegible]PowerShell[illegible]Windows 7[illegible]Windows 8[illegible]6[illegible]9[illegible]

[illegible]

□□ □□1□□□□□□□□□□□CloudShare.com□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CloudShare□□□□□□□Windows□□

1□□Shell□□□□□□□□□□□□

2□□□□□□□□□□□□□□□□□□□□□□□□□□□$session□□□□

3□□□$session□□□□□□□□□□□□□□□□□□□Shell□□□

4□ □Invoke-Command□□□$session□□□□□□□□□□□□□□□□□□□

5□□□Invoke-command□Get-PSSession□□□□□□□□□□□□□20□□□□□□□□□□□□

6□□□Invoke-Command□$session□□□□□□□□□□□ServerManager□□□

7□□ServerManager□□□□□□□□□□□□□□□□□□□□□“rem”□□□□□□□□□□□□

8□□□□□□□□Get-WindowsFeature□□□

9□□□□□□$session□□□□□□□

□□□ □□□PowerShell v3□□□□□□□□□□□□Import-Module□□□□□□□□6□□□7□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

20.8 □□□□□

□□□□□□□□□□□□□□□□PowerShell□□□□Exchange Server? SharePoint Server? VMware vSphere? System Center Virtual Machine Manager?□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□

[illegible]21[illegible] [illegible]

[illegible]PowerShell[illegible]
[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]——[illegible]

21.1 [illegible]

[illegible]Windows[illegible].BAT[illegible].CMD[illegible]Windows[illegible]cmd.exe Shell[illegible]

PowerShell[illegible]——[illegible]——[illegible]Shell[illegible]PowerShell ISE[illegible]PowerGUI[illegible]PrimalScript[illegible]PowerShell Plus[illegible]

ISE[illegible]Shell[illegible]ISE[illegible]“[illegible]”[illegible]“[illegible]”[illegible]

21.2 [illegible]

PowerShell[illegible]WMI[illegible]

[illegible]PowerShell ISE[illegible]ISE[illegible]ISE[illegible]

[illegible]

[illegible]

```
Get-WmiObject -class Win32_LogicalDisk -computername localhost
➥ -filter "drivetype=3" |
 Sort-Object -property DeviceID |
 Format-Table -property DeviceID,
 @{label='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as [int]}},
 @{label='Size(GB';expression={$_.Size / 1GB -as [int]}},
 @{label='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

> **[illegible]** [illegible]name[illegible]label[illegible]n[illegible]l[illegible]L[illegible]1[illegible]

[illegible]21.1[illegible]ISE[illegible]“[illegible]”[illegible]Shell[illegible]ISE[illegible]Cmdlet[illegible]

[illegible]F5[illegible]ISE[illegible]F8[illegible]

[illegible]——[illegible]Get-DiskInventory.ps1[illegible] “[illegible]-[illegible]”[illegible]Cmdlet[illegible]Cmdlet[illegible]Cmdlet[illegible]

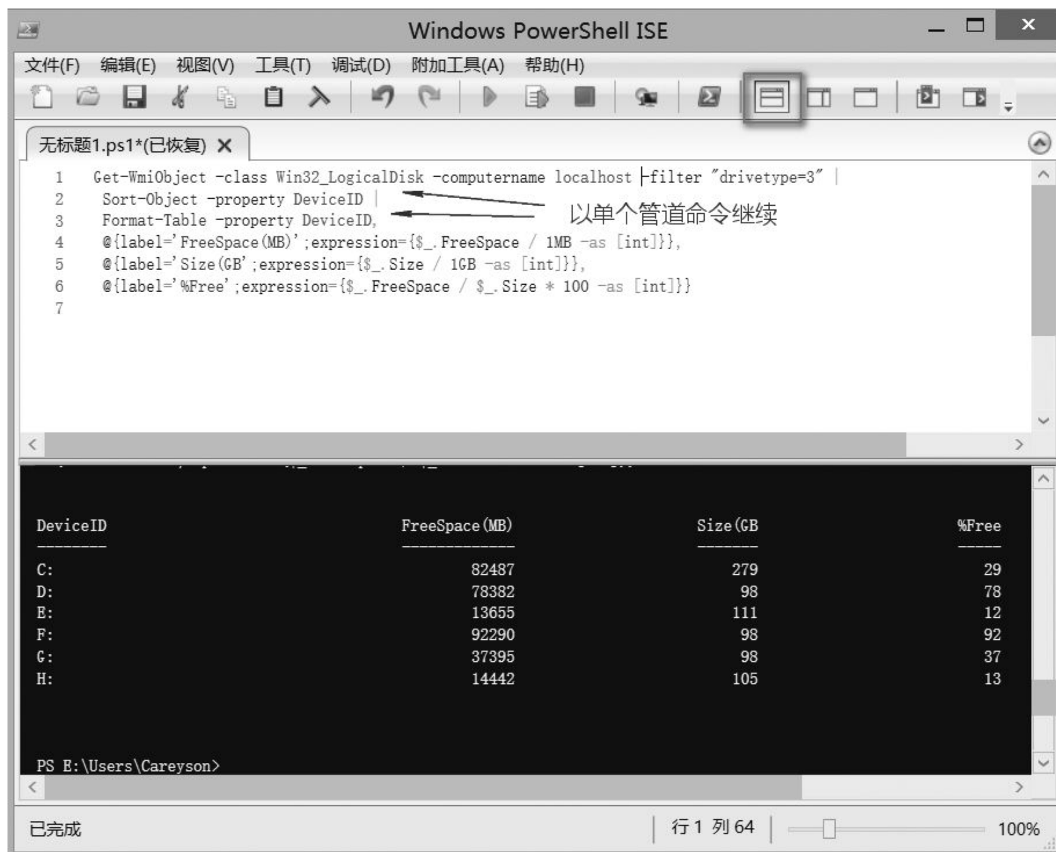


图21.1 [illegible]ISE[illegible]

[illegible]14[illegible]17[illegible]PowerShell[illegible]

21.3 [illegible]

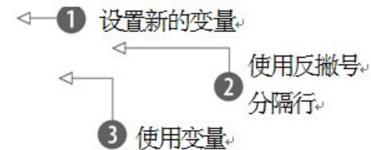
[illegible]Get-DiskInventory.ps1[illegible]PowerShell[illegible]

[illegible]-computer-name[illegible]

□□

□□□□21.1 Get-DiskInventory.ps1□□□□□□□□□

```
$computername = 'localhost'
Get-WmiObject -class Win32_LogicalDisk `
 -computername  $computername `
 -filter "drivetype=3" |
 Sort-Object -property DeviceID |
 Format-Table -property DeviceID,
     @{label='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as [int]}},
     @{label='Size(GB';expression={$_.Size / 1GB -as [int]}},
     @{label='%Free';expression={$_.FreeSpace / $_.Size * 100 -as [int]}}
```



□□□□□□□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□$computername□□□□□□localhost ❶□□□□□□□□□PowerShell□□□□□□-computerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$computername□
- □□□-computerName□□□□□□□□□□□□❸□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□localhost□□□$computerName□□□
- □□□-computerName□□□□□□□□□□□□❷□□□□□□□□□□□□□□PowerShell□□

□□□

21.4 □□□□□□□□□□

□□$computername□□□□□□□□□□□

PowerShell□□□□□□□□□□□□□□

□□□□21.2 Get-DiskInventory.ps1□□□□□□□□

```
param (
  $computername = 'localhost'
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername `
 -filter "drivetype=3" |
 Sort-Object -property DeviceID |
 Format-Table -property DeviceID,
     @{label='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as [int]}},
     @{label='Size(GB';expression={$_.Size / 1GB -as [int]}},
     @{label='%Free';expression={$_.FreeSpace / $_.Size * 100 -as [int]}}
```

❶ 参数块

[illegible]Param()[illegible]❶[illegible]$computerName[illegible]localhost[illegible]

[illegible]

```
PS C:\> .\Get-DiskInventory.ps1 server-r2
PS C:\> .\Get-DiskInventory.ps1 -computername server-r2
PS C:\> .\Get-DiskInventory.ps1 -comp server-r2
```

[illegible]2[illegible]3[illegible]3[illegible]PowerShell[illegible].\[illegible]Shell[illegible]

[illegible]3[illegible]21.3[illegible]

[illegible]21.3 Get-DiskInventory.ps1[illegible]

```
param (
  $computername = 'localhost',
  $drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername `
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Format-Table -property DeviceID,
     @{label='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as [int]}},
     @{label='Size(GB';expression={$_.Size / 1GB -as [int]}},
     @{label='%Free';expression={$_.FreeSpace / $_.Size * 100 -as [int]}}
```

指定额外参数

使用参数

[illegible]PowerShell[illegible]18[illegible]

[illegible]

```
PS C:\> .\Get-DiskInventory.ps1 server-r2 3
PS C:\> .\Get-DiskInventory.ps1 -comp server-r2 -drive 3
PS C:\> .\Get-DiskInventory.ps1 server-r2
PS C:\> .\Get-DiskInventory.ps1 -drive 3
```

[illegible]Param()[illegible]-drivetype[illegible]3[illegible]-computerName[illegible]localhost[illegible]

21.5 [illegible]

[illegible]PowerShell[illegible]Cmdlet[illegible]PowerShell[illegible]

[illegible]21.4[illegible]

[illegible]21.4 [illegible]Get-DiskInventory.ps1[illegible]

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter, free space, total size, and percentage of free
space.
.PARAMETER computername
The computer name, or names, to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk, and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
param (
```

```
  $computername = 'localhost',
  $drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername `
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Format-Table -property DeviceID,
     @{label='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}},
     @{label='Size(GB';expression={$_.Size / 1GB -as [int]}},
     @{label='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

□□□□□□PowerShell□□□□□#□□□□□□□□□□#□□□□□□□□□□□□□□□□<# #>□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□#□

□□□□□□□□□□□□□□□□□□□□□□Help .\Get-DiskInventory□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Cmdlet□□□21.2□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□help .\Get-DiskInventory –full□□□□□□□□□□□□□□□□□□□□□□□21.3□□□□□□□

```
Windows PowerShell

名称
    D:\ps\Get-DiskInventory.ps1

摘要
    Get-DiskInventory retrieves logical disk information from one or
    more computers.


语法
    D:\ps\Get-DiskInventory.ps1 [[-computername] <Object>] [[-drivetype] <Object>] [<CommonParameters>]


说明
    Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
    instances from one or more computers. It displays each disk's
    drive letter, free space, total size, and percentage of free
    space.

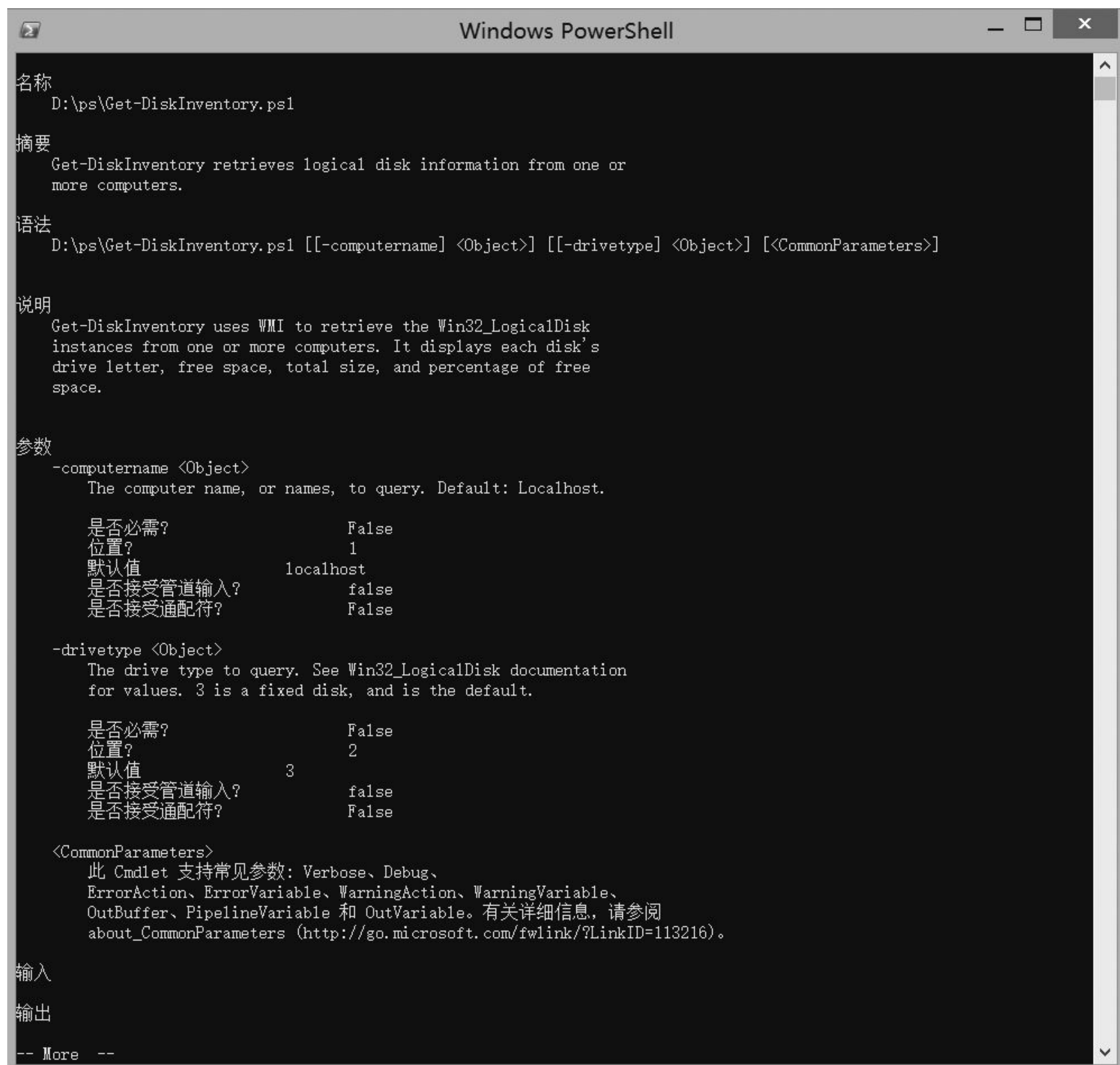

相关链接

备注
    若要查看示例，请键入: "get-help D:\ps\Get-DiskInventory.ps1 -examples".
    有关详细信息，请键入: "get-help D:\ps\Get-DiskInventory.ps1 -detailed".
    若要获取技术信息，请键入: "get-help D:\ps\Get-DiskInventory.ps1 -full".



PS D:\ps>
```

[illegible]21.2 [illegible]



□21.3 □□□□□□-example□-detailed□□-full□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□.DESCRIPTION□.SYNOPSIS□□□□□□□□□□□□□□PowerShell□□□
help about_comment_based _help□□□□□□□□

21.6 □□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□
□□□□□Shell□□□□□□□□□□□□□

□□□□□□□□□

□□□□□□□□□□□

```
Get-Process
Get-Service
```

□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□□□

□□
□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□“□□□□□□□□□□□□”□□21.4 □□□□
□□

□21.4 □□□□□□□□□□□□□□□□□□□□□□□□

□□□
□□□□□

□1□□□Get-Process□

□2□□□□□Process□□□□□□□

□3□□□□Out-Default□□□□□□□□□□□□

□4□Out-Default□□□□□□Out-Host□□□□□□□□□□□□□□□□□□□□□□□
□10□□□□□□□□

□5□□□□□□□□□□□□□□

□6□□□Get-Service□

□7□□□□□Service□□□□□□□

□8□□□□Out-Default□□□□□□□□□□□□

□9□Out-Default□□□□□□Out-Host□□□□□□□□□□□□□□□□□□□□□

□10□□□□□□□□□□□□□□

□□
Test.ps1□□Ctrl+C
□□□□□□□□□□□□

□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□Shell□□
□□□□□□□ISE□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□ISE□□□□□□□□□□□□□□□□□□□□□□

□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□21.5□

□□□□□□□□□□□□

□1□□□□□Get-Process□

□2□□□□□Process□□□□□□□

□3□□□□□Get-Service□

□4□□□□□Service□□□□□□□

□5□□□□Out-Default□□□□□□□□□□□□□□□□

[illegible]6[illegible]Out-Default[illegible]Out-Host[illegible]

[illegible]7[illegible]Process[illegible]Shell[illegible]Process[illegible]Process[illegible]Shell[illegible]Service[illegible]

[illegible]8[illegible]

[illegible]PowerShell[illegible]

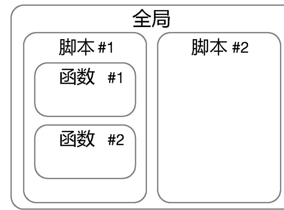
[illegible]21.5 [illegible]

21.7 [illegible]

[illegible]scope[illegible]PowerShell[illegible]

Shell[illegible]global scope[illegible]script scope[illegible]child[illegible]parent[illegible]private scope[illegible]

[illegible]21.6[illegible]



[illegible]21.6 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]——[illegible]

[illegible]

[illegible]

[illegible]1[illegible]PowerShell[illegible]PowerShell ISE[illegible]

[illegible]2[illegible]PowerShell[illegible]PowerShell ISE[illegible]

[illegible]3[illegible]ISE[illegible]Write $x[illegible]

[illegible]4[illegible]c:\scope.ps1[illegible]

[illegible]5[illegible]PowerShell[illegible]C:\Scope[illegible]$x[illegible]PowerShell[illegible]——[illegible]$x[illegible]PowerShell[illegible]$x[illegible]

[illegible]6[illegible]PowerShell[illegible]$x[illegible]C:\Scope[illegible]$x[illegible]PowerShell[illegible]

[illegible]7[illegible]ISE[illegible]$x=10[illegible]write[illegible]

[illegible]8[illegible]PowerShell[illegible]C:\Scope[illegible]10[illegible]$x[illegible]Shell[illegible]Shell[illegible]$x[illegible]4[illegible]

[illegible]PowerShell[illegible]New-Alias Dir Get-Service[illegible]Dir[illegible]Get-Service[illegible]Get-ChildItem[illegible]Shell[illegible]Shell[illegible]Dir[illegible]Dir[illegible]Dir[illegible]

[illegible]Param()[illegible]

21.8 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]Help[illegible]

[illegible]

```
Get-WmiObject Win32_LogicalDisk -comp "localhost" -filter
"drivetype=3" |
Where { $_.FreeSpace / $_.Size -lt .1 } |
Select -Property DeviceID,FreeSpace,Size
```

[illegible]2[illegible]10%[illegible]1[illegible]3[illegible]3[illegible]

[illegible]22[illegible] [illegible]

[illegible]——[illegible]

22.1 [illegible]

[illegible]22.1[illegible]

[illegible]22.1 [illegible]Get-DiskInventory.ps1

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter[illegible] free space[illegible] total size[illegible] and percentage of free
space.
.PARAMETER computername
The computer name[illegible] or names[illegible] to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk[illegible] and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
param (
  $computername = 'localhost'[illegible]
  $drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
```

```
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
     @{name='Size(GB';expression={$_.Size / 1GB -as [int]}}□
     @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

[illegible]Select-Object[illegible]Format-Table[illegible]CSV[illegible]

```
PS C:\> .\Get-DiskInventory | Format-Table
```

[illegible]CSV[illegible]

```
PS C:\> .\Get-DiskInventory | Export-CSV disks.csv
```

[illegible]Select-Object[illegible]

22.2 [illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]“[illegible]”[illegible]PowerShell[illegible]22.2[illegible]——[illegible]

[illegible]22.2 [illegible]Get-DiskInventory.ps1[illegible]

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter□ free space□ total size□ and percentage of free
space.
.PARAMETER computername
The computer name□ or names□ to query. Default: Localhost.
.PARAMETER drivetype
```

```
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk□ and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
[CmdletBinding()]
param (
  $computername = 'localhost'□
  $drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
     @{name='Size(GB';expression={$_.Size / 1GB -as [int]}}□
     @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

□□□□□□□□□□□□□□□[CmdletBinding()]□□□□□□□□□□□□□□□□PowerShell□□□

22.3 □□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□-ComputerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□——□□□□□□□□□□□□□□□□□□□□□□□□□□22.3□□□

□□□□22.3 □Get-DiskInventory.ps1□□□□□□□□

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter□ free space□ total size□ and percentage of free
space.
.PARAMETER computername
```

```
The computer name□ or names□ to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk□ and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
[CmdletBinding()]
param (
  [Parameter(Mandatory=$True)]
  [string]$computername□

  [int]$drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
     @{name='Size(GB)';expression={$_.Size / 1GB -as [int]}}□
     @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□“comp”□□□□□□□□□□□□□□□□□“ComputerName”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□

□□□□□□□□□□□□□

```
[Parameter(Mandatory=$True□HelpMessage="Enter a computer name
to query")
```

□□PowerShell□□□

[illegible]

[illegible][Parameter(Mandatory=$True)][illegible]PowerShell[illegible]PowerShell[illegible]-computerName[illegible][string][illegible]-drivetype[illegible]INT[illegible]

[illegible]Param()[illegible]22.1[illegible]

```
param (
  [Parameter(Mandatory=$True)]
  [string]$computername,
  [int]$drivetype = 3
)
```


[illegible]22.1 [illegible]Param()[illegible]

[illegible]

- [illegible]Param()[illegible]
- [illegible]22.1[illegible]Mandatory[illegible]-computerName——[illegible]-drivetype[illegible]
- [illegible]
- [illegible]Param()[illegible]
- [illegible]——$computername[illegible]$drivetype——[illegible]PowerShell[illegible]-computername[illegible]-drivetype[illegible]

[illegible]22.3[illegible]Shell[illegible]-computername[illegible]PowerShell[illegible]

22.4 [illegible]

[illegible]“computername”[illegible]-computerName[illegible]PowerShell[illegible]Get-Service[illegible]Get-WmiObject[illegible]Get-Process[illegible]-computerName[illegible]

[illegible]-hostname[illegible]22.4[illegible]

[illegible]22.4 [illegible]Get-DiskInventory.ps1[illegible]

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter□ free space□ total size□ and percentage of free
space.
.PARAMETER computername
The computer name□ or names□ to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk□ and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
[CmdletBinding()]
param (
  [Parameter(Mandatory=$True)]
  [Alias('hostname')]
  [string]$computername□

  [int]$drivetype = 3
)
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
```

```
     @{name='Size(GB';expression={$_.Size / 1GB -as [int]}}□
     @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> .\Get-DiskInventory -host SERVER2
```

□□□ □□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□-host□□□PowerShell□□□□□-hostname□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□-computerName□□□□□□□□□□□□-drivetype□□□□□□□□-computerName□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
[Parameter(Mandatory=$True)][Alias('hostname')]
[string]$computername□
```

□□□□□□□□□□□□□□□□□□□□

22.5 □□□□□□□□

□□□□□-drivetype□□□□□□□□□□MSDN□WIN32_LogicalDisk□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□3□□□□□□□□2□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□1□4□5□6□□□□□□□□□□□□□□□□□□□6□RAM□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□22.5□□□□□□□□□□□□□□□□□

□□□□□22.5 □Get-DiskInventory.ps1□□□□□□

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter□ free space□ total size□ and percentage of free
```

```
space.
.PARAMETER computername
The computer name□ or names□ to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk□ and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
[CmdletBinding()]
param (
  [Parameter(Mandatory=$True)]
  [Alias('hostname')]
  [string]$computername□

  [ValidateSet(2□3)]
  [int]$drivetype = 3

)
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
     @{name='Size(GB';expression={$_.Size / 1GB -as [int]}}□
     @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
```

□□□□□□PowerShell□□□□□-drivetype□□□□□□□2□3□□□□3□□□□□

□□□help about_functions_advanced_parameters□□□□□□□□——□□□□□□□□□□ValidateSet□Jeffery□□□□□□□□□□□□□□“□□”□□□□□□□——□□□□□□http://jdhitsolutions.com/blog/ □□□□□□□□□□□□“validate”□□

□□□□□□□□□□□□□□□□□□——□□□□-drivetype□□□5□□□PowerShell□□□□□□□

22.6 □□□□□□□□□□□□□□□

□□19□□□□□□□□□□□□□□Write-Verbose□□□Write-Host□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□22.6□□□□□□□□□

□□□□22.6 □Get-DiskInventory.ps1□□□□□

```
<#
.SYNOPSIS
Get-DiskInventory retrieves logical disk information from one or
more computers.
.DESCRIPTION
Get-DiskInventory uses WMI to retrieve the Win32_LogicalDisk
instances from one or more computers. It displays each disk's
drive letter□ free space□ total size□ and percentage of free
space.
.PARAMETER computername
The computer name□ or names□ to query. Default: Localhost.
.PARAMETER drivetype
The drive type to query. See Win32_LogicalDisk documentation
for values. 3 is a fixed disk□ and is the default.
.EXAMPLE
Get-DiskInventory -computername SERVER-R2 -drivetype 3
#>
[CmdletBinding()]
param (
  [Parameter(Mandatory=$True)]
  [Alias('hostname')]
  [string]$computername□

  [ValidateSet(2□3)]
  [int]$drivetype = 3
)
Write-Verbose "Connecting to $computername"
Write-Verbose "Looking for drive type $drivetype"
Get-WmiObject -class Win32_LogicalDisk -computername $computername
`
 -filter "drivetype=$drivetype" |
 Sort-Object -property DeviceID |
 Select-Object -property DeviceID□
     @{name='FreeSpace(MB)';expression={$_.FreeSpace / 1MB -as
[int]}}□
     @{name='Size(GB';expression={$_.Size / 1GB -as [int]}}□
```

```
    @{name='%Free';expression={$_.FreeSpace / $_.Size * 100 -as
[int]}}
Write-Verbose "Finished running command"
```

[illegible]

```
PS C:\> .\Get-DiskInventory -computername localhost
```

[illegible]

```
PS C:\> .\Get-DiskInventory -computername localhost –verbose
```

[illegible]——[illegible]

[illegible]——[illegible]-Verbose[illegible][CmdletBinding()][illegible]Write-Host[illegible]$VerbosePreference[illegible]

[illegible]PowerShell[illegible]$computername[illegible]PowerShell[illegible]

22.7 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]12[illegible]——[illegible]21[illegible]-ComputerName[illegible]hostname[illegible]——[illegible]

[illegible]

```
get-wmiobject win32_networkadapter -computername localhost |
 where { $_.PhysicalAdapter } |
 select MACAddress,AdapterType,DeviceID,Name,Speed
```

[illegible]

- [illegible]
- [illegible]
- [illegible]-ComputerName[illegible]
- [illegible]hostname[illegible]
- [illegible]
- [illegible]
- [illegible]Get-PhyscialAdapters.ps1[illegible]

[illegible]23[illegible] [illegible]

[illegible]13[illegible]PowerShell[illegible]——[illegible]

[illegible]PowerShell v3[illegible]1[illegible]

23.1 [illegible]

[illegible]13[illegible]PowerShell[illegible]session configurations[illegible]64[illegible]32[illegible]PowerShell[illegible]64[illegible]PowerShell[illegible]64[illegible]PowerShell[illegible]

[illegible]

```
PS C:\> Get-PSSessionConfiguration

Name           : microsoft.powerShell
PSVersion      : 3.0
StartupScript  :
RunAsUser      :
Permission     : NT AUTHORITY\NETWORK AccessDenied,
BUILTIN\Administrators
                  AccessAllowed
Name           : microsoft.powerShell.workflow
PSVersion      : 3.0
StartupScript  :
RunAsUser      :
Permission     : NT AUTHORITY\NETWORK AccessDenied,
BUILTIN\Administrators
                  AccessAllowed

Name           : microsoft.powerShell32
PSVersion      : 3.0
```

```
StartupScript  :
RunAsUser      :
Permission     : NT AUTHORITY\NETWORK AccessDenied,
BUILTIN\Administrators
                  AccessAllowed
```

□□□□□□□□□□□□□□□□□□“Microsoft.PowerShell”□□□□□□□□
New-PSSession □Enter-PSSession □Invoke-Command□□□□□□□
□□□□□□□64□□□□□□□□64□□Shell□□32□□□
□□“Microsoft.PowerShell”□32□□Shell□

□□□□□□□□□□64□□□□□□□32□Shell□□□□
□□“Microsoft.PowerShell32”□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□-ConfigurationName□□□□□□□□□□

```
PS C:\> Enter-PSSession -ComputerName DONJONES1D96 -
ConfigurationName 'Micr
osoft.PowerShell32'
[DONJONES1D96]: PS C:\Users\donjones\Documents>
```

□□□□□□□□□□□□□□□□□□□□□□□□□32□□PowerShell□□□□□□□□□
□□□□□□32□□□□□□□□□□□64□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□

23.2 □□□□□□

□□□□□□□□□□□□□□□□□□

□1□□□New-PSSessionConfigurationFile□□□□□□□□□□□□□□□
□□□□□□□□PSSC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□2□□□Register-PSSessionConfiguration□□□.PSSC□□□□□
WinRm□□
□□□□□□□Set-PSSessionConfiguration□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□
□□□□□□□□□□□□□□HelpDesk□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□——□□□□□□□□□□□□□□□□□HelpDesk□□□□□□□□□□□□□□□□□□

HelpDesk

23.2.1

——

```
PS C:\> New-PSSessionConfigurationFile
  -Path C:\HelpDeskEndpoint.pssc
  -ModulesToImport NetAdapter
  -SessionType RestrictedRemoteServer
  -CompanyName "Our Company"
  -Author "Don Jones"
  -Description "Net adapter commands for use by help desk"
  -PowerShellVersion '3.0'
```

- -**Path**; .pssc
- -**ModulesToImport**; NetAdapter
- -**SessionType RestrictedRemoteServer**; PowerShell Select-Object Measure-Object Get-Command Get-Help Exit-PSSession
- -**PowerShellVersion**; 3.0

-Visible -VisibleCmdlets -ModulesToImport Cmdlet visibility Cmdlet VisibleCmdlets Cmdlets ——

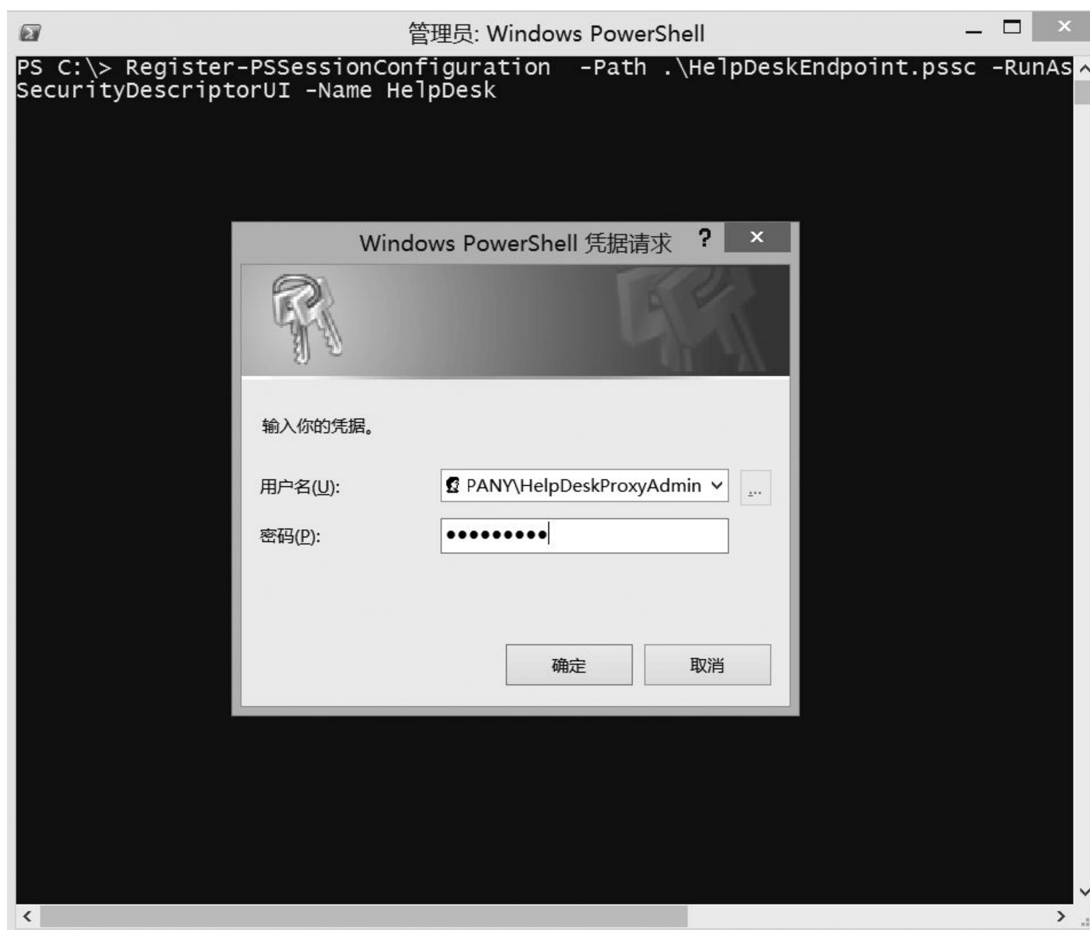
PowerShell Visual Studio

23.2.2 [illegible]

[illegible]

```
PS C:\> Register-PSSessionConfiguration
  -Path .\HelpDeskEndpoint.pssc
  -RunAsCredential COMPANY\HelpDeskProxyAdmin
  -ShowSecurityDescriptorUI
  -Name HelpDesk
```

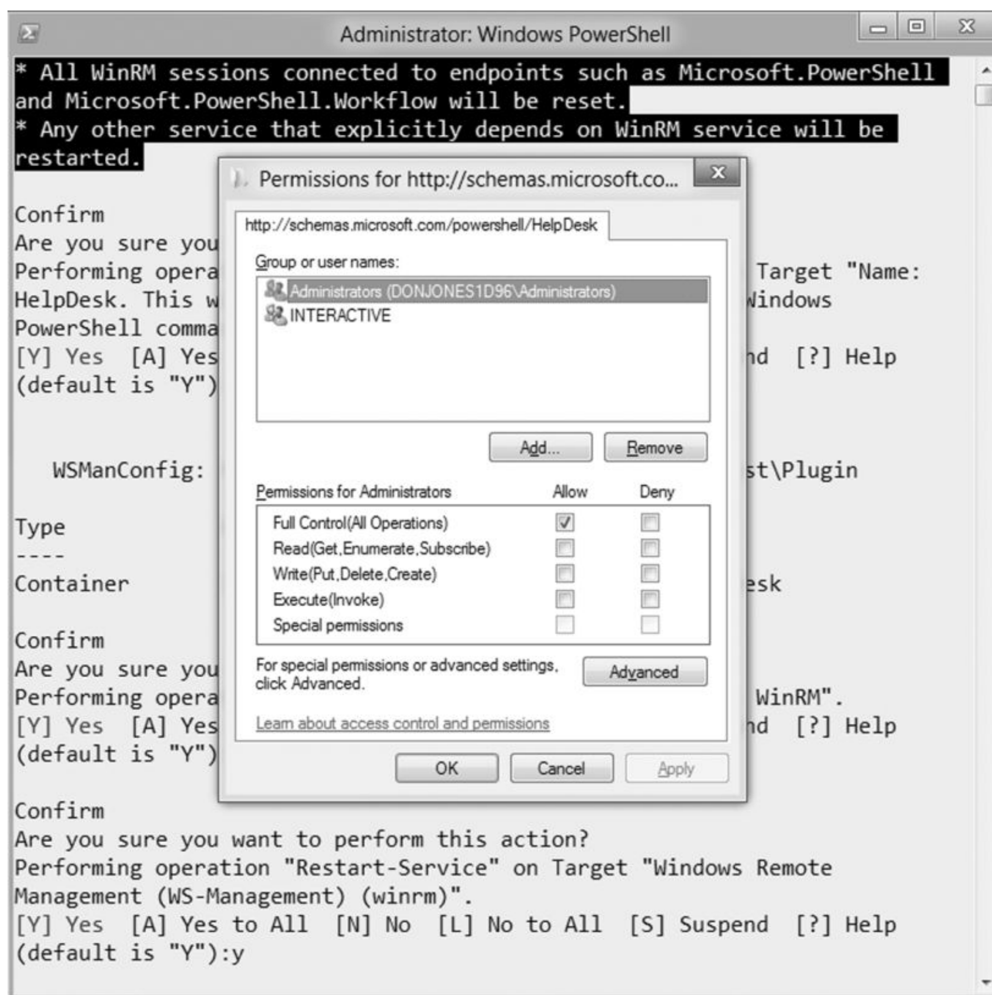
[illegible]HelpDesk[illegible]23.1[illegible]COMPANY\HelpDeskProxyAdmin[illegible]



[illegible]23.1 [illegible]

[illegible]“[illegible]”[illegible]WinRM[illegible]

[illegible]23.2[illegible]-ShowSecurityDescriptorUI[illegible]SDDL[illegible]Shell[illegible]GUI[illegible]——[illegible]HelpDesk[illegible]



[illegible]23.2 [illegible]

[illegible]

```
PS C:\> Enter-PSSession -ComputerName DONJONES1D96 -
ConfigurationName HelpD
```

```
esk
[DONJONES1D96]: PS>Get-Command

Capability   Name
ModuleN

ame
----------   ----                                              -
------
CIM           Disable-NetAdapter
NetA...
CIM           Disable-NetAdapterBinding
NetA...
CIM           Disable-NetAdapterChecksumOffload
NetA...
CIM           Disable-NetAdapterEncapsulatedPacketTaskOffload
NetA...
CIM           Disable-NetAdapterIPsecOffload
NetA...
CIM           Disable-NetAdapterLso
NetA...
CIM           Disable-NetAdapterPowerManagement
NetA...
CIM           Disable-NetAdapterQos
NetA...
CIM           Disable-NetAdapterRdma
NetA...
CIM           Disable-NetAdapterRsc
NetA...
CIM           Disable-NetAdapterRss
NetA...
CIM           Disable-NetAdapterSriov
NetA...
CIM            Disable-NetAdapterVmq
NetA...
CIM           Enable-NetAdapter
NetA...
CIM           Enable-NetAdapterBinding
NetA...
CIM           Enable-NetAdapterChecksumOffload
NetA...
CIM            Enable-NetAdapterEncapsulatedPacketTaskOffload
NetA...
CIM            Enable-NetAdapterIPsecOffload
NetA...
CIM            Enable-NetAdapterLso
NetA...
CIM            Enable-NetAdapterPowerManagement
```

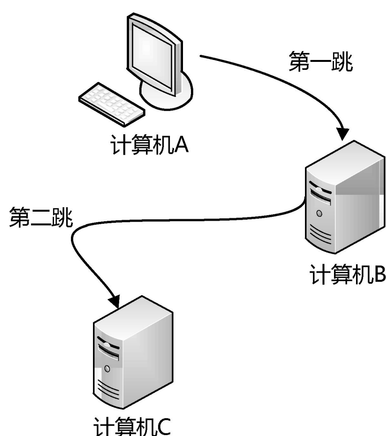
```
NetA...
CIM            Enable-NetAdapterQos
NetA...
```

□□□PowerShell□□□□□□□□□PowerShell□□□GUI□□

23.3 □□□□□□multi-hop remoting□

□□□□□□□13□□□□□□□□□□□□□□□□□□□□23.3□□□“□□□”□“□□”□□□□□□□□A□□□□□□□□□□PowerShell□□□□□□□□B□□□□□□□□□□□□□□□□□□□□□□□□□□□B□□□□□□□□□□□□□□□□□C□□□□□□□

□□□□□PowerShell□□□□□□□A□□□□□□B□□□□□□□□□□□□□□□□B□□□□□□□□□□□□□□□□□□□□□□□□□B□□C□



□23.3 □Windows PowerShell□□□□□□

□Windows Vista□□□□□□□□□□□□□□□□□□□□□□□□□

□1□□□□□□□□□□□□□A□□□□□Enable-WSManCredSSP-RoleClient– DelegateComputer x□□□□x□□*□□□□□□□□□□□□□□□□□□□□□□□□□□*.company.com□

[illegible]2[illegible]B[illegible]Enable-WSManCredSSP–Role Server[illegible]

[illegible]Enable-WSManCredSSP[illegible]Don[illegible]“Secrets of PowerShell Remoting guide”[illegible]

23.4 [illegible]

[illegible]PowerShell[illegible]Enter-PSSession –computerName DC01[illegible]DC01[illegible]DC01[illegible]

[illegible]Domain Name System[illegible]DNS[illegible]DC01[illegible]IP[illegible]DNS[illegible]DC01[illegible]IP[illegible]——[illegible]IP[illegible]DC01[illegible]——[illegible]——[illegible]

23.4.1 [illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]

- [illegible]IP[illegible]
- [illegible]

[illegible]DC01.COMPANY .LOC[illegible]IP[illegible]DNS[illegible]CNAME[illegible]SSL[illegible]“[illegible]”[illegible]

23.4.2 □□SSL□□□□□□

□□SSL□□□□□□□□□□□□SSL□□Enter-PSSession –computerNameDC01.COMPANY.LOC -UseSSL -credential COMPANY\Administrator□□□□□□DC01□□□□□□□□□“dc01.company.loc”□□□□□□□□□□□□□□□-credential□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□Microsoft Management Console□MMC□□□MMC□□□□□SSL□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□HTTP□□□Don□Secrets of PowerShell Remoting guide□□□□□□□□□□□□□□□□□□□□□□□□

23.4.3 □□□□□□□□□□□□

□□□□□□SSL□□□“□□□□□□□□□□□□□□□□□□□□□□□□□DNS□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□“*.COMPANY. COM”□□□Company.com□□□□□□□□

□□

□□□GPO□□□□□□□□□□□□□□□□□□□□

□1□□□□□□□□□

□2□□□□□□□□□

□3□□□Windows□□□

□4□□□Windows□□□□□

□5□□□WinRM□□□□

□6□□□□□□□□□□

□7□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□“*.company.com,*.sales.company.com.”□

□□□□□Windows□□□PowerShell□□□□□□□□□□□Shell□□□help about_remote_troubleshooting□□□□□

□□□-Credential□□——□□□□□□□□□□□□□□□□□

23.5 □□□□

□□□ □□□□□□□□□□□□□□□□PowerShell v3□□□□□PowerShell□□□□□

□□□□□□□□□□□□□TestPoint□□□□□□□□□□□□SmbShare□□□□□□□□□□□□□□□Get-SmbShare□□□□□□□□□□□Exit-PSSession□□□Cmdlet□□□□□□□□□□□□□PowerShell Cmdlet□

□□Enter-PSSession□□□localhost□□□□□□□□TestPoint□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Get-Command□□□□□□□□□□□□□□□□□□□□□□

□□□ □□□□□□□□□□Windows 8□Windows Server 2012□□□□□□□Windows□□□——SmbShare□□□□□□□□□□□Windows□□□□□

□24□ □□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□□□□□□□□□□□□□□regular expression□□regex□□□□□□□□□□□□□□□□□□□□□Unix□Linux□□□□□□□□□Power Shell□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□IIS□□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□

□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□Shell□□□□□□□□□

24.1 □□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□IPv4□□□1□3□□□□□□□□□□4□□□□□□□□□□□□□□□□□□□□□□□□□□211.193.299.299□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□——□□Web□□□□□□□□□□□□HTTP 500□□□□□□□□□□□SMTP□□

24.2 □□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□“Don”□□□□□□□□□□□□□□□□□□□□□PowerShell□□□“DON”“don”“Don”“DoN”□——PowerShell□□□□□□□□□□□□□□□

[illegible]

- \w [illegible]“[illegible]”[illegible]\won[illegible]“Don”“Ron”[illegible]“ton”[illegible]\w[illegible]
- \W [illegible] \w [illegible]PowerShell[illegible]——[illegible]“[illegible]”[illegible]
- \d [illegible]0[illegible]9[illegible]
- \D [illegible]
- \s [illegible]Tab[illegible]
- \S [illegible]
- .[illegible]
- [abcde][illegible]d[aeiou]n[illegible]“Don”“Dan”[illegible]“Doun”[illegible]“Deen”[illegible]
- [a-z][illegible][a-f,m-z][illegible]
- [^abcde] [illegible]d[^aeiou][illegible]“dns”[illegible]“don”[illegible]
- [illegible]do?n[illegible]“don”[illegible]“doon”[illegible]“dn”[illegible]
- * [illegible]do*n[illegible]“doon”[illegible]“don”[illegible]“dn”[illegible]*[illegible]
- + [illegible]dn[illegible]+o[illegible]“dndndndno”[illegible]“dn”[illegible]
- \[illegible].[illegible]\[illegible]
- {2}[illegible]\d{1}[illegible]1[illegible]2[illegible]2[illegible]{1[illegible]3}[illegible]1[illegible]3[illegible]
- ^[illegible]d.n[illegible]“don”[illegible]“pteranodon”[illegible]^d.n[illegible]“don”[illegible]“pteranodon”[illegible]^[illegible]^[illegible][][illegible]

- $□□□□□□□□□□□□□□□□□□□□.icks□□□□“hicks”□□□□□□□“sticks”□□□□□□□□□□□“ticks”□□□□□□□□“Dickson”□□□□□□□□□.icks$□□□□“Dickson”□□□□□□□□$□□□“s”□□□□□□□□□□□□□□□

□□□

- \d{1,3}.\d{1,3}.\d{1,3}.\d{1,3} □□□□IPv4□□□□□□□□□□□□□□□“432.567.875.000”□□□□□□□□□□□□□“192.169.15.12”□□□□□□□□
- \\\w+(\\w+)+□□□□□□□□□□□UNC□□
- \w{1}.\w+@company.com□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□“@company.com”□□□d.jones@company.com□□□□□□□□□□□□□□“donald.jones@company.com.org”□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□^□$□

□□□ □□□□PowerShell□□help about_regular_expressions□□□

24.3 □□-Match□□□□□

PowerShell□□□□□□□□□-Match□□□□□□□□□□□□□-Cmatch□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> "don" -match "d[aeiou]n"
True
PS C:\> "dooon" -match "d[aeiou]n"
False
PS C:\> "dooon" -match "d[aeiou]+n"
True
PS C:\> "djinn" -match "d[aeiou]+n"
False
PS C:\> "dean" -match "d[aeiou]n"
False
```

[illegible]-Match[illegible]True[illegible]False[illegible]

[illegible]-Match[illegible]Shell[illegible]-Match[illegible]

24.4 [illegible]Select-String[illegible]

[illegible]IIS[illegible]IIS[illegible]PowerShell[illegible]……[illegible]

[illegible]zip[illegible] http://MoreLunches.com [illegible]Web[illegible]IISlog[illegible]C:\Logfiles[illegible]WSSVC1[illegible]WSSVC2[illegible]WSSVC3[illegible]

[illegible]40x[illegible]“[illegible]”[illegible]Web[illegible]HTTP[illegible]“401”[illegible]“error401.html”[illegible]\s40[0-9]\s[illegible]40x[illegible]400[illegible]499[illegible]

```
PS C:\logfiles> get-childitem -filter *.log -recurse | select-
string -pattern
      "\s40[0-9]\s" | format-table Filename,LineNumber,Line –wrap
```

[illegible]C:\logfiles[illegible].log[illegible]Select-String[illegible]MatchInfo[illegible]Format-Table[illegible]Web[illegible]

[illegible]Gecko[illegible]

Windows NT6.2[illegible]user-agnet[illegible]

```
(Windows+NT+6.2;+WOW64;+rv:11.0)+Gecko
```

[illegible]64[illegible]User-agent[illegible]“WOW64”[illegible]6.2;[\w\W]++Gecko ——[illegible]

- 6\.2[illegible]——[illegible]“6.2”[illegible]
- [\w\W]+ ——[illegible]——[illegible]
- +Gecko ——[illegible]“Gecko”[illegible]

[illegible]

```
PS C:\logfiles> get-childitem -filter *.log -recurse | select-
string -pattern
      "6\.2;[\w\W]+\+Gecko"

W3SVC1\u_ex120420.log:14:2012-04-20 21:45:04 10.211.55.30 GET
/MyApp1/
      Testpage.asp - 80 - 10.211.55.29 Mozilla/
      5.0+
(Windows+NT+6.2;+WOW64;+rv:11.0)+Gecko/20100101+Firefox/11.0 200 0
0
      1125
W3SVC1\u_ex120420.log:15:2012-04-20 21:45:04 10.211.55.30 GET
/TestPage.asp-
      80 - 10.211.55.29 Mozilla/5.0+
(Windows+NT+6.2;+WOW64;+rv:11.0)+Gecko/
      20100101+Firefox/11.0 200 0 0 1 109
```

[illegible]Cmdlet[illegible]

[illegible]IIS[illegible]Windows[illegible]Message[illegible]ID[illegible]4624[illegible]ID[illegible]Windows[illegible]Windows Server 2008 R2[illegible]“WIN”[illegible]

[illegible]TM20$[illegible]TM40$[illegible]WIN[\W\w]+TM[234][0-9]\$ ——[illegible]$[illegible][\W\w][illegible]\w[illegible]

```
PS C:\> get-eventlog -LogName security | where { $_.eventid -eq 4624 } |
      select -ExpandProperty message | select-string -pattern
      "WIN[\W\w]+TM[234][0-9]\$"
```

[illegible]Where-Object[illegible]ID[illegible]4624[illegible]Message[illegible]Select-String[illegible]

```
PS C:\> get-eventlog -LogName security | where { $_.eventid -eq 4624 -and
      $_.message -match "WIN[\W\w]+TM[234][0-9]\$" }
```

[illegible]Message[illegible]Message[illegible]——[illegible]Event[illegible]

24.5 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]——[illegible]

- [illegible]2[illegible]
- [illegible]ID[illegible]Get-Process[illegible]Get-Member[illegible]
- [illegible]Windows Update[illegible]C:\Windows[illegible]

24.6 [illegible]

PowerShell Shell

- Switch
- Cmdlets
- -Match —— $matches

PowerShell Jeffrey E.F. Friedl *Mastering Regular Expressions* by Jeffrey (O’Reilly) Windows .NET PowerShell

http://RegExLib.com IP http://RegExTester.com

[illegible]25[illegible] [illegible]

[illegible]

25.1 Profile[illegible]Shell[illegible]

[illegible]PowerShell[illegible]PSDrives[illegible]Shell[illegible]

25.1.1 PowerShell Profile[illegible]

[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell[illegible]PowerShell ISE[illegible]PowerShell[illegible]PowerShell[illegible]Shell[illegible]Profile[illegible]

[illegible]Profile[illegible]PowerShell[illegible]——[illegible]SnapIn[illegible]Don[illegible]Profile[illegible]

```
Import-Module ActiveDirectory
Add-PSSnapIn SqlServerCmdletSnapIn100
Cd C:\
```

[illegible]Profile[illegible]Don[illegible]Shell[illegible]C[illegible]——C[illegible]Don[illegible]Profile[illegible]

> [illegible] [illegible]ActiveDirectory[illegible]AD:PSDrive[illegible]Don[illegible]Shell[illegible]AD:PSDrive[illegible]

[illegible]PowerShell[illegible]Profile[illegible]Profile[illegible]Help About_Profiles[illegible]PowerShell[illegible]PowerShell ISE[illegible]Profile[illegible]

□□□Profile□□□□□□□□□□□□□Profile□□□□□□□□□□Profile□□□□□□□□□□□□ISE□□□□□□——□□□□□□□□□□□□□□□□□□ISE□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□1□$PsHome/Profile.PS1——□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$PSHome□□□□□□□□□□PowerShell□□□□□□PowerShell□□□□□□□□□□□

□2□$PsHome/Microsoft.PowerShell_Profile.PS1——□□□PowerShell□ISE□□□$PsHome/Microsoft.PowerShellISE_Profile.ps1□□□□□□□

□3□$Home/Documents/WindowsPowerShell/Profile.PS1 ——□□

□4□$Home/Documents/WindowsPowerShell/Microsoft.PowerShell_Profile.ps1——□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□PowerShell ISE□□□□□□ $Home/Documents/WindowsPowerShell/Microsoft.PowerShellISE_Profile.PS1□

□□

□64□□□□□□□□□□□□□□32□□64□□PowerShell□□□□□□□□□□□32□□64□□□□□□□□□□□□□□□□32□□64□PowerShell□□32□□Profile□□□□□64□□□□□□32□□PowerShell□□□□□□□□□□□□□

□□□□About_Profiles□□

- $PsHome□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□C:\Windows\System32\WindowsPowerShell\V1.0□□□64□□□□□□64□□□PowerShell□□
- $Home□□□□□□□□□□□□□□□□□□□□□□□□□□□□C:\Users\Administrator□□

- □□□□□□□□□□□□“Documents”□□□□□□□□□□□□□□□□Windows□□□□□□“My Documents”□
- □□□□□□□□□“□□□□□□□□□□□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ISE□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□Shell□□□□□□□PowerShell□□□□□□□□□□□ISE□□□□□□□□□□$Home\Documents\WindowsPowerShell\Profile1.PS1——□□□Profile□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□Profile□□□□□□□□□□□□□□□□□□□□□□□□□□“It Worked”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Shell□□□ISE□□□□□□□□□□□Shell□□□ISE□□□□Profile□□□□□□□

□□□□Profile□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□Restricted□□□Profile□□□□□□□□□□□□□□□□□□AllSigned□□□□□Profile□□□□□□□□□□□□□□□17□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□17□□□□□□

25.1.2 □□□□□

PowerShell□□——□□□□□□□□□□□PS C:\>□□□□□□□□□□□□□□Prompt□□Profile□□□□□□□□□□□□□□□□□□□□□□Shell□□□□□□□□□□□□□□□□□

□□□□□□□□□□□

```
Function Prompt
{
     $(IF (Test-Path Variable:/PSDebugContext) { '[DBG]: ' }
     ELSE { '' }) + 'PS ' + $(Get-Location) `
     + $(IF ($NestedPromptLevel -Ge 1) { '>>' }) + '> '
}
```

□□□□□□□□$DebugContext□□□□□□□□□PowerShell□Variable:Drive□□□□□□□□□□□□□□[DBG]:□□□□□□□□□□□□□□□□□□□□□PS□□□□Get-Location Cmdlet□□□□□□□□□□PS D:\Test>□□□□□

Shell[illegible]——[illegible]$NestedPromptLevel[illegible]“>>”[illegible]

[illegible]Profile[illegible]Shell[illegible]

```
Function Prompt {
 $Time = (Get-Date).ToShortTimeString()
 "$Time [$ENV:COMPUTERNAME]:> "
}
```

[illegible]

```
6:07 PM [CLIENT01]:>
```

[illegible]PowerShell[illegible]——PowerShell[illegible]$Time[illegible]

25.1.3 [illegible]

[illegible]Shell[illegible]Don[illegible]——[illegible]PowerShell[illegible]

[illegible]PowerShell[illegible]“[illegible]”[illegible]“[illegible]”[illegible]25.1[illegible]



[illegible]25.1 [illegible]Shell[illegible]

[illegible] Profile[illegible]PowerShell[illegible]

```
(Get-Host).PrivateData.ErrorForegroundColor="Green"
```

[illegible]

- ErrorForegroundColor
- ErrorBackgroundColor
- WarningForegroundColor
- WarningBackgroundColor
- DebugForegroundColor
- DebugBackgroundColor
- VerboseForegroundColor

- VerboseBackgroundColor
- ProgressForegroundColor
- ProgressBackgroundColor

□□□□□□□□□□□□□□

- Red
- Yellow
- Black
- White
- Green
- Cyan
- Magenta
- Blue

□□□□□□□□□□□□□□□□□□□DarkRed□DarkYellow□DarkGreen□DarkCyan□DarkBlue□□

25.2 □□□□-AS,-IS,-Replace,-Join,-Split,-IN,-Contains

□□

25.2.1 –AS□–IS

-AS□□□Converting□Casting□□□□□□□□□□□□□

```
1000/3 –AS [INT]
```

□□□□□□□□□□□□□□□□□□□□□□□-AS□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□[String]□[XML]□[INT]□[Single]□[Double]□[Datetime]□□

-IS[illegible]True[illegible]False[illegible]

```
123.45 -IS [INT]
"SERVER-R2" -IS [String]
$True -IS [Bool]
(Get-Date) -IS [DateTime]
```

[illegible]

25.2.2 –Replace

-Replace[illegible]

```
PS C:\> "192.168.34.12" -Replace "34","15"
192.168.15.12
```

[illegible]-Replace[illegible]“34”[illegible]“15”[illegible]

25.2.3 –Join[illegible]-Split

-Join[illegible]-Split[illegible]

[illegible]5[illegible]

```
PS C:\> $Array = "one","two","three","four","five"
PS C:\> $Array
one
two
three
four
five
```

[illegible]PowerShell[illegible]-Join[illegible]

```
PS C:\> $Array -Join "|"
one|two|three|four|five
```

[illegible]

```
PS C:\> $String = $Array -Join "|"
PS C:\> $String
one|two|three|four|five
PS C:\> $String | Out-File Data.DAT
```

[illegible]-Split[illegible]

```
PS C:\>Gc Computers.tdf
Server1 Windows East Managed
```

[illegible]Gc[illegible]Get-Content[illegible]

[illegible]-Split[illegible]4[illegible]

```
PS C:\> $Array = (Gc Computers.tdf) -Split "`t"
PS C:\> $Array
Server1
Windows
East
Managed
```

[illegible]“t”(`t)[illegible]PowerShell[illegible]

[illegible]4[illegible]

```
PS C:\> $Array[0]
Server1
```

25.2.4 –Contains[illegible]-IN

-Contains[illegible]PowerShell[illegible]

```
PS C:\> 'this' -Contains '*his*'
False
```

[illegible]-like[illegible]

```
[illegible]PS C:\> 'this' -Like '*his*'
True
```

-Like[illegible]-Contains[illegible]

```
PS C:\> $Collection = 'abc','def','ghi','jkl'
PS C:\> $Collection -Contains 'abc'
True
PS C:\> $Collection -Contains 'xyz'
False
```

-IN[illegible]

```
PS C:\> $Collection = 'abc','def','ghi','jkl'
PS C:\> 'abc' -IN $Collection
True
PS C:\> 'xyz' -IN $Collection
False
```

25.3 [illegible]

[illegible]

[illegible]PowerShell[illegible]Methods[illegible]Gm[illegible]

```
PS C:\> "Hello" | Gm

   TypeName: System.String
Name       MemberType    Definition
--------     ------------   ----------------
```

```
Clone      Method      System.ObjectClone()
CompareTo    Method      int CompareTo(System.Object value...
Contains     Method      bool Contains(string value)
CopyTo      Method      System.VoidCopyTo(intsourceInde...
EndsWith     Method      bool EndsWith(string value), bool...
Equals      Method      bool Equals(System.Objectobj), b...
GetEnumerator   Method      System.CharEnumeratorGetEnumerat...
GetHashCode    Method      int GetHashCode()
GetType     Method      type GetType()
GetTypeCode    Method      System.TypeCodeGetTypeCode()
IndexOf     Method      int IndexOf(char value), intInde...
IndexOfAny    Method      int IndexOfAny(char[] anyOf), int...
Insert      Method      string Insert(intstart Index, str...
IsNormalized   Method      bool IsNormalized(), bool IsNorma...
LastIndexOf    Method      int LastIndexOf(char value), int ...
LastIndexOfAny  Method      int LastIndexOfAny(char[] anyOf),...
Normalize    Method      string Normalize(), string Normal...
PadLeft     Method      string PadLeft(int totalWidth), s...
PadRight     Method      string PadRight(int totalWidth), ...
Remove      Method      string Remove(int startIndex, int...
Replace     Method      string Replace(char oldChar, char...
Split      Method      string[] Split(Params char[] sepa...
StartsWith    Method      bool StartsWith(string value), bo...
Substring    Method      string Substring(int startIndex),...
ToCharArray    Method      char[] ToCharArray(), char[] ToCh...
ToLower     Method      string ToLower(), string ToLower(...
ToLowerInvariant Method      string ToLowerInvariant()
ToString     Method      string ToString(), string ToStrin...
ToUpper     Method      string ToUpper(), string ToUpper(...
ToUpperInvariant Method      string ToUpperInvariant()
Trim       Method      string Trim(Params char[] trimCha...
TrimEnd     Method      string TrimEnd(Params char[] trim...
TrimStart    Method      string TrimStart(Params char[] tr...
Chars      ParameterizedProperty char Chars(int index) {get;}
Length      Property     System.Int32 Length {get;}
```

[illegible]String[illegible]

- IndexOf()[illegible]

```
PS C:\> "SERVER-R2".IndexOf("-")
6
```

- Split()[illegible]Join()[illegible]Replace()[illegible]-Split[illegible]-Join[illegible]-Replace[illegible] [illegible]PowerShell[illegible]String[illegible]

- ToLower()□ToUpper()□□□□□□□□□□□□□□□

```
PS C:\> $ComputerName = "SERVER17"
PS C:\> $ComputerName.tolower()
server17
```

- Trim()□□□□□□□□□□□□□□□TrimStart()□TrimEnd()□□□□□□□□□□
  □□□□□□□□□□

```
PS C:\> $UserName = "Don"
PS C:\> $UserName.Trim()
Don
```

□□□□□□□□□□□□□□String□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ToLower()□Trim()□□□□□□□□□□□□□□□□□□□□□□□□IndexOf()□□□□

25.4 □□□□

□String□□□□□□□Date(□□□□□□□□□□DateTime)□□□

```
PS C:\>Get-Date | Gm

   TypeName: System.DateTime

Name          MemberType   Definition
-------        -----------   ------------
Add         Method     System.DateTimeAdd(System.TimeSpan ...
AddDays       Method     System.DateTimeAddDays(double value)
AddHours       Method     System.DateTimeAddHours(double value)
AddMilliseconds    Method
System.DateTimeAddMilliseconds(doub...
AddMinutes      Method     System.DateTimeAddMinutes(double va...
AddMonths      Method     System.DateTimeAddMonths(int months)
AddSeconds      Method     System.DateTimeAddSeconds(double va...
AddTicks       Method     System.DateTimeAddTicks(long value)
AddYears       Method     System.DateTimeAddYears(int value)
CompareTo      Method     intCompareTo(System.Object value), ...
Equals        Method     boolEquals(System.Object value), bo...
GetDateTimeFormats   Method     string[] GetDateTimeFormats(),
strin...
```

```
GetHashCode      Method     intGetHashCode()
GetType       Method     type GetType()
GetTypeCode      Method     System.TypeCodeGetTypeCode()
IsDaylightSavingTime Method     bool IsDaylightSavingTime()
Subtract       Method     System.TimeSpanSubtract(System.Date...
ToBinary       Method     long ToBinary()
ToFileTime      Method     long ToFileTime()
ToFileTimeUtc     Method     long ToFileTimeUtc()
ToLocalTime      Method     System.DateTimeToLocalTime()
ToLongDateString    Method     string ToLongDateString()
ToLongTimeString    Method     string ToLongTimeString()
ToOADate       Method     double ToOADate()
ToShortDateString   Method     string ToShortDateString()
ToShortTimeString   Method     string ToShortTimeString()
ToString       Method     string ToString(), string ToString(s...
ToUniversalTime    Method     System.DateTimeToUniversalTime()
DisplayHint      NoteProperty
Microsoft.PowerShell.Commands.Displa...
Date         Property    System.DateTime Date {get;}
Day         Property    System.Int32 Day {get;}
DayOfWeek      Property    System.DayOfWeekDayOfWeek {get;}
DayOfYear      Property    System.Int32 DayOfYear {get;}
Hour         Property    System.Int32 Hour {get;}
Kind         Property    System.DateTimeKind Kind {get;}
Millisecond      Property    System.Int32 Millisecond {get;}
Minute        Property    System.Int32 Minute {get;}
Month        Property    System.Int32 Month {get;}
Second        Property    System.Int32 Second {get;}
Ticks        Property    System.Int64 Ticks {get;}
TimeOfDay      Property    System.TimeSpan TimeOfDay {get;}
Year         Property    System.Int32 Year {get;}
DateTime       ScriptProperty System.ObjectDateTime {get=if ((&
{...
```

[illegible]DateTime[illegible]

```
PS C:\> (Get-Date).Month
10
```

[illegible]DateTime[illegible]90[illegible]AddDays()[illegible]

```
PS C:\> $Today=Get-Date
PS C:\> $90DaysAgo=$Today.AddDays(-90)
PS C:\> $90DaysAgo
```

```
2014□12□19□ 9:36:47
```

□□□□“To”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\> $90DaysAgo.ToShortDateString()
2014/12/19
```

□□□□□□□□□□□□□□□□□□□□□□□□□□——□□□□□□□□□□□□□□□

25.5 □□WMI□□

□WMI□□□□□□□□□□□□□□□□□□□□Win32_OperatingSystem□□□□□□□□□□□□□□□□□□□□□□□□□□

```
PS C:\>Get-WMIObject Win32_OperatingSystem | Select LastBootUpTime

LastBootUpTime
--------------
20150317090459.125599+480
```

PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□WMI□□□□□□□□□□□WMI□□□□□□□□Gm□□□□□□□□□□□□

```
PS C:\>Get-WMIObject Win32_OperatingSystem | Gm
   TypeName:
System.Management.ManagementObject#root\cimv2\Win32_OperatingS
ystem

Name         MemberType   Definition
------        -------------  ----------
Reboot        Method     System.Management...
SetDateTime      Method     System.Management...
Shutdown       Method     System.Management...
Win32Shutdown     Method     System.Management...
Win32Shutdown Tracker  Method     System.Management...
BootDevice      Property    System.String Boo...
...
PSStatus       PropertySet   PSStatus {Status,...
ConvertFromDateTime  ScriptMethod  System.Object Con...
ConvertToDateTime   ScriptMethod  System.Object Con...
```

[illegible]ConvertFrom DateTime()[illegible]ConvertToDateTime()[illegible]WMI[illegible]

```
PS C:\> $OS=Get-WMIObject Win32_OperatingSystem
PS C:\> $OS.ConvertToDateTime($OS.LastBootUpTime)

2015□3□17□ 9:04:59
```

[illegible]Select-Object[illegible]Format-Table[illegible]

```
PS C:\> Get-WMIObject Win32_OperatingSystem |Select
BuildNumber,_Server,@{
l='LastBootTime';E={$_.ConvertToDateTime($_.LastBootUpTime)}}

BuildNumber              __Server                  LastBootTime
-----------             ---------                 ------------
7601                       SERVER-R2                  2015/3/17
9:04:59
```

25.6 [illegible]

[illegible]PowerShell[illegible]Dir[illegible]-Path[illegible]PowerShell[illegible]——[illegible]

[illegible]$PSDefaultParameterValues[illegible]PowerShell[illegible]Profile[illegible]

[illegible]-Credential[illegible]

```
PS C:\> $Credential = Get-Credential -UserName Administrator -
Message
"Enter Admin Credential"
PS C:\> $PSDefaultParameterValues.Add('*:Credential',$Credential)
```

[illegible]Invoke-Command Cmdlet[illegible]Get-Credential[illegible]

```
PS C:\>$PSDefaultParameterValues.Add('Invoke-Command:Credential',
{Get-Credential -Message 'Enter Administrator Credential' –UserName
Administrator})
```

[illegible]Add()[illegible]<Cmdlet>:<Parameter>[illegible]<Cmdlet>[illegible]*[illegible]Add()[illegible]

[illegible]$PSDefaultParameterValues[illegible]

```
PS C:\>$PSDefaultParameterValues

Name              Value
-------            -------
*:Credential         System.Management.Automation.PSCredenti
Invoke-Command:Credential    Get-Credential -Message 'Enter
administ
```

[illegible]

PowerShell[illegible]Scope[illegible]21[illegible]

[illegible]$PSDefaultParameterValues[illegible]Shell[illegible]>$PSDefaultParameterValues[illegible]Shell[illegible]

[illegible]“[illegible]”[illegible]About_Scope[illegible]

[illegible]PowerShell[illegible]About_Parameters_Default_Values[illegible]

25.7 [illegible]

[illegible]PowerShell[illegible]

- Where-Object[illegible]-FilterScript[illegible]
- ForEach-Object[illegible]-Process[illegible]
- [illegible]Select-Object[illegible]Format-Table[illegible]E[illegible]Expression[illegible]
- [illegible]
- [illegible]Job[illegible]Invoke-Command[illegible]Start-Job[illegible]-ScriptBlock[illegible]

[illegible]——[illegible]@[illegible]&[illegible]

```
PS C:\> $Block = {
>> Get-Process | Sort -Property Vm -Descending | Select -First 10 }
>>
PS C:\>&$Block

Handles  NPM(K)  PM(K)   WS(K)  VM(M)  CPU(s)  Id  ProcessName
-------   -----   -----    -----  -----   ------  ---  ------------
---
   680    42    14772     13576   1387     3.84    404  svchost
   454    26   68368     75116     626     1.28   1912 powerShell
   396     37   179136    99252     623     8.45   2700 powerShell
   497     29    15104      6048     615    0.41   2500
SearchIndexer
   260    20     4088      8328     356     0.08   3044 taskhost
   550    47    16716     13180     344     1.25   1128 svchost
  1091     55    19712     35036     311     1.81   3056 explorer
   454    31    56660     15216     182    45.94  1596 MsMpEng
   163    17    62808     27132     162     0.94   2692 dwm
   584    29     7752      8832     159     1.27    892  svchost
```

[illegible]PowerShell[illegible]About_Script_Block[illegible]

25.8 [illegible]

[illegible]PowerShell[illegible]

[illegible]Twitter[illegible]too-@jeffhicks[illegible]@concentrateddon[illegible]Twitter[illegible]PowerShell.Org[illegible]PowerShell[illegible]

[illegible]26[illegible] [illegible]

[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]http://PoshCode.org[illegible]PowerShell[illegible]

[illegible]Christoph Tohermes[illegible]Kaia Taylor[illegible]

[illegible]PowerShell[illegible]

26.1 [illegible]

[illegible]26.1[illegible]New-WebProject.ps1[illegible]IIS Cmdlet——[illegible]Cmdlet[illegible]Web[illegible]Windows Server 2008 R2[illegible]

[illegible]26.1 New-WebObject.ps1

```
param(
  [parameter(Mandatory = $true)]
  [string] $Path,
  [parameter(Mandatory = $true)]
  [string] $Name
  )
$System = [Environment]::GetFolderPath("System")
$script:hostsPath = ([System.IO.Path]::Combine($System,
"drivers\etc\"))
➥+"hosts"
```

```
function New-localWebsite([string] $sitePath, [string] $siteName)
{
 try
 {
  Import-Module WebAdministration
 }
 catch
 {
 Write-Host "IIS PowerShell module is not installed. Please
install it
➥first, by adding the feature"
}
Write-Host "AppPool is created with name: " $siteName
New-WebAppPool -Name $siteName
Set-ItemProperty IIS:\AppPools\$Name managedRuntimeVersion v4.0
Write-Host
if(-not (Test-Path $sitePath))
{
  New-Item -ItemType Directory $sitePath
  }
  $header = "www."+$siteName+".local"
  $value = "127.0.0.1 " + $header
  New-Website -ApplicationPool $siteName -Name $siteName -Port 80
➥-PhysicalPath $sitePath -HostHeader ($header)
  Start-Website -Name $siteName
  if(-not (HostsFileContainsEntry($header)))
  {
   AddEntryToHosts -hostEntry $value
  }
 }

 function AddEntryToHosts([string] $hostEntry)
 {
  try
  {
   $writer = New-Object System.IO.StreamWriter($hostsPath, $true)
   $writer.Write([Environment]::NewLine)
   $writer.Write($hostEntry)
  $writer.Dispose()
 }
 catch [System.Exception]
 {
  Write-Error "An Error occured while writing the hosts file"
 }
}
function HostsFileContainsEntry([string] $entry)
{
 try
```

```
 {
  $reader = New-Object System.IO.StreamReader($hostsPath +
"hosts")
  while(-not($reader.EndOfStream))
  {
   $line = $reader.Readline()
   if($line.Contains($entry))
   {
    return $true
   }
  }
  return $false
 }
 catch [System.Exception]
 {
  Write-Error "An Error occured while reading the host file"
 }
}
```

[illegible]21[illegible]

```
param(
  [parameter(Mandatory = $true)]
  [string] $Path,
  [parameter(Mandatory = $true)]
  [string] $Name
  )
```

[illegible]-Path[illegible]-Name[illegible]

[illegible]

```
$System = [Environment]::GetFolderPath("System")
$script:hostsPath = ([System.IO.Path]::Combine($System,
"drivers\etc\"))
➡+"hosts"
```

[illegible]——[illegible]GetFolderPath[illegible]Shell[illegible]

```
PS C:\> $system = [Environment]::GetFolderPath('System')
PS C:\> $system
```

```
C:\Windows\system32
PS C:\> $script:hostsPath = ([System.IO.Path]::Combine
($system,"drivers\etc\"))+"hosts"
PS C:\> $hostsPath
C:\Windows\system32\drivers\etc\hosts
PS C:\>
```

$script:hostsPath [illegible] $system [illegible]

[illegible] 3 [illegible] New-LocalWebsite [illegible] AddEntryToHosts [illegible] HostsFile ContainsEntry [illegible] Param() [illegible] Parameter() [illegible]

[illegible] New-LocateWebSite [illegible] HostsFileContainsEntry [illegible]

```
if(-not (HostsFileContainsEntry($header)))
 {
  AddEntryToHosts -hostEntry $value
 }
```

[illegible] AddEntryToHoses [illegible] IF [illegible] PowerShell [illegible] Help *IF* [illegible]

```
PS C:\> help *IF*

Name               Category  Module

----               --------  ------
diff               Alias
New-ModuleManifest        Cmdlet   Microsoft.PowerShell.Core
Test-ModuleManifest         Cmdlet   Microsoft.PowerShell.Core
Get-AppxPackageManifest      Function  Appx
Get-PfxCertificate         Cmdlet   Microsoft.PowerShell.S...
Export-Certificate         Cmdlet   PKI
Export-PfxCertificate        Cmdlet   PKI
```

```
Get-Certificate          Cmdlet   PKI
Get-CertificateNotificationTask   Cmdlet   PKI
Import-Certificate        Cmdlet   PKI
Import-PfxCertificate        Cmdlet   PKI
New-CertificateNotificationTask   Cmdlet   PKI
New-SelfSignedCertificate     Cmdlet   PKI
Remove-CertificateNotification...  Cmdlet   PKI
Switch-Certificate        Cmdlet   PKI
Test-Certificate         Cmdlet   PKI
about_If              HelpFile
```

HelpFile□□□□□□□□□□□□About-If□□□□□□□□□□□□□□□□□□□□IF□□□□□□□□□□□□□□□□□□□□□□□□□□HostsFileContainsEntry□□□□□True□□False□□□□□False□□□□□□AddEntryToHosts□□□□□New-LocalWebSite□□□□□□“□□□”□□□□□□□□□□□□□□□□□□□□□□□□HostsFileContainsEntry □AddEntryToHosts□□□□□□□□□New-LocalWebSite□□□□□——□□□□□□□□□□□□□□□□□□□□New-LocalWebSite□□□

```
function New-localWebsite([string] $sitePath, [string] $siteName)
{
 try
 {
  Import-Module WebAdministration
 }
 catch
 {
  Write-Host "IIS PowerShell module is not installed. Please
install it
➥first, by adding the feature"
 }
 Write-Host "AppPool is created with name: " $siteName
 New-WebAppPool -Name $siteName
 Set-ItemProperty IIS:\AppPools\$Name managedRuntimeVersion v4.0
 Write-Host
 if(-not (Test-Path $sitePath))
 {
  New-Item -ItemType Directory $sitePath
 }
 $header = "www."+$siteName+".local"
 $value = "127.0.0.1 " + $header
 New-Website -ApplicationPool $siteName -Name $siteName -Port 80
➥-PhysicalPath $sitePath -HostHeader ($header)
 Start-Website -Name $siteName
```

```
 if(-not (HostsFileContainsEntry($header)))
 {
  AddEntryToHosts -hostEntry $value
 }
}
```

[illegible]Try[illegible]Help *Try*[illegible]About_Try_Cacth_Finally[illegible]Try[illegible]Catch[illegible]WebAdministration[illegible]WebAdministration[illegible]WebAdministration[illegible]

Write-Host[illegible]New-WebAppPool[illegible]WebAdministration[illegible]Set-ItemProperty[illegible]AppPool[illegible]

[illegible]Write-Host[illegible]Test-Path[illegible]New-Item[illegible]

[illegible]$Header[illegible]$SiteName[illegible]“www.sitename.local” [illegible]$Value[illegible]IP[illegible]New-WebSite[illegible]——[illegible]

[illegible]Start-WebSite[illegible]HostsFileContainsEntry[illegible]AddEntryToHosts[illegible]$Value[illegible]IP[illegible]-[illegible]Hosts[illegible]

26.2 [illegible]

[illegible]

- [illegible]

- [illegible]Get-[illegible]——[illegible]——[illegible]
- [illegible][Environment][illegible]

[illegible]"[illegible]"[illegible]

26.3 [illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]

[illegible]26.2[illegible]

[illegible]PowerShell[illegible]

[illegible] 26.2 Get-LastOn.ps1

```
function get-LastOn {
<#
.DESCRIPTION
Tell me the most recent event log entries for logon or logoff.
.BUGS
Blank 'computer' column

.EXAMPLE
get-LastOn -computername server1 | Sort-Object time -Descending |
Sort-Object id -unique | format-table -AutoSize -Wrap
ID          Domain      Computer   Time
--          ------      --------   ----
LOCAL SERVICE    NT AUTHORITY         4/3/2012 11:16:39 AM
NETWORK SERVICE   NT AUTHORITY         4/3/2012 11:16:39 AM
SYSTEM       NT AUTHORITY         4/3/2012 11:16:02 AM
```

```
Sorting -unique will ensure only one line per user ID, the most
recent.
Needs more testing

.EXAMPLE
PS C:\Users\administrator> get-LastOn -computername server1 -
newest 10000
-maxIDs 10000 | Sort-Object time -Descending |

Sort-Object id -unique | format-table -AutoSize -Wrap

ID         Domain    Computer  Time
--         ------    --------  ----
Administrator   USS          4/11/2012 10:44:57 PM
ANONYMOUS LOGON  NT AUTHORITY      4/3/2012 8:19:07 AM
LOCAL SERVICE   NT AUTHORITY      10/19/2011 10:17:22 AM
NETWORK SERVICE  NT AUTHORITY      4/4/2012 8:24:09 AM
Student     WIN7          4/11/2012 4:16:55 PM
SYSTEM      NT AUTHORITY      10/18/2011 7:53:56 PM
USSDC$      USS          4/11/2012 9:38:05 AM
WIN7$      USS          10/19/2011 3:25:30 AM

PS C:\Users\administrator>

.EXAMPLE
get-LastOn -newest 1000 -maxIDs 20
Only examines the last 1000 lines of the event log

.EXAMPLE
get-LastOn -computername server1| Sort-Object time -Descending |
Sort-Object id -unique | format-table -AutoSize -Wrap
#>

param (
         [string]$ComputerName = 'localhost',
         [int]$Newest = 5000,
         [int]$maxIDs = 5,
         [int]$logonEventNum = 4624,
         [int]$logoffEventNum = 4647
      )

      $eventsAndIDs = Get-EventLog -LogName security -Newest
$Newest |
      Where-Object {$_.instanceid -eq $logonEventNum -or
➥$_.instanceid -eq $logoffEventNum} |
      Select-Object -Last $maxIDs
➥-Property TimeGenerated,Message,ComputerName
```

```
      foreach ($event in $eventsAndIDs) {
         $id = ($event |
         parseEventLogMessage |
         where-Object {$_.fieldName -eq "Account Name"} |
         Select-Object -last 1).fieldValue

         $domain = ($event |
         parseEventLogMessage |
         where-Object {$_.fieldName -eq "Account Domain"} |
         Select-Object -last 1).fieldValue

         $props = @{'Time'=$event.TimeGenerated;
              'Computer'=$ComputerName;
              'ID'=$id
              'Domain'=$domain}

         $output_obj = New-Object -TypeName PSObject -Property
$props
         write-output $output_obj
      }
}

function parseEventLogMessage()
{
      [CmdletBinding()]
      param (
         [parameter(ValueFromPipeline=$True,Mandatory=$True)]
         [string]$Message
      )

      $eachLineArray = $Message -split "`n"

      foreach ($oneLine in $eachLineArray) {
         write-verbose "line:_$oneLine_"
         $fieldName,$fieldValue = $oneLine -split ":", 2
              try {
                   $fieldName = $fieldName.trim()
                   $fieldValue = $fieldValue.trim()
              }
              catch {
                   $fieldName = ""
              }

              if ($fieldName -ne "" -and $fieldValue -ne "" )
              {
              $props = @{'fieldName'="$fieldName";
                        'fieldValue'=$fieldValue}
```

```
              $output_obj = New-Object -TypeName PSObject -
Property $props
              Write-Output $output_obj
              }
      }
}
Get-LastOn
```

□27□　□□□□

□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□PowerShell□□□

27.1　□□□□□□□□

□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□Exchange□SharePoint□□□□□□□

□□ToolMaking□□——□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□

- PowerShell□□□□□□□□
- □□□□
- □□□□□□□□□□□□□□□□□□□□□□□
- □□□□□
- □□□□□□□□
- □□□
- □□□□□□□□
- □□□□□□□□
- □□□□□□□□
- □□□□□□
- □□□□
- □□□□□
- □□□□□□□□□□
- □□□□□□□□□□

- [illegible]PowerShell[illegible]
- [illegible]
- [illegible]
- .Net[illegible]

[illegible]PowerShell[illegible]——[illegible]PowerShell[illegible]PowerShell[illegible]

27.2 [illegible]

[illegible]PowerShell[illegible]

[illegible]

- [illegible]
- [illegible]PowerShell[illegible]NTFS[illegible]PowerShell[illegible]Cacls.exe[illegible]Xcacls.exe[illegible]PowerShell[illegible]Get-ACL[illegible]Set-ACL[illegible]
- [illegible]Exchange[illegible]——[illegible]
- [illegible]Windows Server 2008 R2[illegible]WebAdministration[illegible]IIS[illegible]Windows Server 2008[illegible]IIS7[illegible]

[illegible]“[illegible]”[illegible]Don[illegible]PowerShell[illegible]Web Server[illegible]Don[illegible]“[illegible]XCopy[illegible]RoboCopy[illegible]”[illegible]Don[illegible]“[illegible]PowerShell[illegible]”[illegible]“PowerShell[illegible]”[illegible]

27.3 [illegible]

PowerShell PowerShell
PowerShell ——
PowerShell ——

- MoreLunches.com——
- http://PowerShell.org——Don
- http://jdhitsolutions.com/blog——Jeff
  PowerShell
- http://mcpmag.com/Articles/List/Prof-PowerShell.aspx
  ——Jeff MCP Mag.Com “Prof.PowerShell”
- http://PowerShell.org——PowerShell Q&A
  PowerShell

http://PowerShellBooks.org/wp/books
Learn PowerShell Toolmaking in a Month of
Lunches PowerShell In Depth Manning

PowerShell
http://CBTNuggets.com Don PowerShell
MoreLunches.com

□28□ PowerShell□□□□

□□□

28.1 □□□□

□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
PowerShell□□□□□□□□□□□□□□□□□□□PowerShell□□□□□

- `□□□□□——□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□cd C:\Program Files□□□□□□□□□□□□□□□□□□cd Program` Files□□□
- ~□□□□□——□□~□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□UserProfile□□□□□
- ()□□□□——□□□□□□□□

-□□□□□□□□□□□□□□□□□□□□PowerShell□□□Get-Service –ComputerName (Get-Content C:\ComputerNames.txt)□

-□□Change-Start-Mode('Audomatic')□□Delete()□

- []□□□□□——□PowerShell□□□□□□□□□

-□□□$Services[2]□□□$Services□□□□□□□□□□□□□□□□□□0□□□□□□

-□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$My Result/3 as [INT]□□□□□□□□□□□□□□□□□□□□□[XML]$Data=Get-Content Data.XML□□□Data.XML□□□□□□□□□□□□□□□□□□□XML□□□

- {}[illegible]——[illegible]

-[illegible]Script Blocks[illegible]Get-Service | Where-Object{$_.Status –eq 'Running'}[illegible]

-[illegible]-[illegible]“@”[illegible]-[illegible]-[illegible]$HashTable= @{l='Label';e={expression}}[illegible]

-[illegible]${My Variable}[illegible]

- ' '[illegible]——[illegible]String[illegible]PowerShell[illegible]
- " "[illegible]——[illegible]PowerShell[illegible]$[illegible]$[illegible]$One[illegible]“World”[illegible]$Two="Hello $One `n"[illegible]$Two[illegible]“Hello World”[illegible]`n[illegible]
- $[illegible]——[illegible]PowerShell $[illegible]Cmdlet[illegible]$One[illegible]Two[illegible]New-Variable –Name $One –Value 'Hello'[illegible]Two[illegible]“Hello”——[illegible]Two[illegible]$[illegible]PowerShell[illegible]$One[illegible]New-Variable –Name One –Value 'Hello'[illegible]One[illegible]
- %[illegible]——[illegible]ForEach-Object Cmdlet[illegible]
- ?[illegible]——[illegible]Where-Object Cmdlet[illegible]
- >[illegible]——[illegible]Out-File Cmdlet[illegible]Cmd.exe[illegible]Dir>Files.Txt[illegible]
- + - * / %[illegible]——[illegible]+[illegible]
- -[illegible]——[illegible]-Co
- mputerName[illegible]-Eq[illegible]Cmdlet[illegible]Get-Content[illegible]

- @□at□□□——□PowerShell□□□□□□

  -□□□□□□□□□□□□□□□□□□□□□□□□□

  -□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$Array= @(1,2,3,4)□□□□@□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□

  -□□□□□Here-String□Here-String□□□□□□□□□□□□□□□□□□□□□□Here-String□“@”□□□□□□□□□□□□□□□□□“@”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Help About_Quoting_Rules□□□□□□□□□□□Here-String□□□□□□□□□□□□□

  -@□□PowerShell□□□□□□Splat Operator□□Cmdlet□Don□□□TechNet Magazine□□□□□□□□□□Splating□□□□□https://technet.microsoft.com/en-us/magazine/gg675931.aspx□□

- &□□□□□——□□PowerShell□□□□□□□□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□$a="Dir"□□□“Dir”□□□□□$a□□□&$a□□□□Dir□□□
- ;□□□□——□□□□□□□□PowerShell□□□□□□□□□□□Dir;Get-Process□□□□□□□□□□Dir□□□□□□□Get-Process□□□□□□□□□□□□□□□□□□□□□□□Dir□□□□□□□□□□□□□□□□□□Get-Process□□□
- #□□□□——□□□□□□□□□□□□#□□□□□□□□□□□□□□□□□□□□PowerShell□□□□□□□<>□□□□□□□□□□□□□□□□□□□“<#”□□□□□“#>”□□□□□□□□□□□□□□□□□□□□□□□□PowerShell□□□□
- =□□□□——□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□$One=1□□□□□□□□□□□□□□□□□□□□□-Eq□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$Var+=5□□□□□□$Var□□□□□□5□
- |□□□□□——□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□Cmdlet□□□□Cmdlet□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□9□□□□□□□□□□□□□
- \□□/□□□□□□□□□——□□□C:\Windows□C:/Windows□□□□□□□□□□WMI□□□□□□□□□□□□□□□□□□□□□□□□□

- .[illegible]——[illegible]

-[illegible]$_.Status[illegible]$_[illegible]Status[illegible]

-[illegible]“.”[illegible].C:\myscript.ps1[illegible]

-[illegible]“.”[illegible]..[illegible]“..”[illegible]..\[illegible]

- ,[illegible]——[illegible]"One",2,"Three",4[illegible]Get-Process –ComputerName Server1,Server2,Server3[illegible]
- :[illegible]——[illegible].Net FrameWork[illegible][DateTime]::Now[illegible]Get-Date[illegible]
- ![illegible]——[illegible]“[illegible]”(Not)[illegible]

[illegible]PowerShell[illegible]“^”[illegible]

28.2 [illegible]

[illegible]PowerShell[illegible]

- []——[illegible][-Name <String>][illegible][-Name] <String>[illegible][[-Name] <String>][illegible]
- []——[illegible]<String>[][illegible]<String>[illegible]
- <>——[illegible]<String>[illegible]<int>[illegible]<Process>[illegible]

[illegible]Help[illegible]-Full[illegible]
[illegible]

28.3 [illegible]

PowerShell[illegible]

- -eq——[illegible]-ceq[illegible]
- -ne——[illegible]-cne[illegible]
- -ge——[illegible]-cge[illegible]
- -le——[illegible]-cle[illegible]
- -gt——[illegible]-cgt[illegible]
- -lt——[illegible]-clt[illegible]
- -contains——[illegible]True[illegible]$Collection –Contains $Object[illegible]-nocontains[illegible]
- -in——[illegible]True[illegible]$Object –in $Collection[illegible]-noin[illegible]

[illegible]

- -not——[illegible]![illegible]
- -and——[illegible]
- -or——[illegible]

[illegible]

- -Join——[illegible]
- -Split——[illegible]
- -Replace——[illegible]
- -Is——[illegible]True[illegible]$ID –Is [INT][illegible]
- -As——[illegible]$ID –As [INT][illegible]
- ..——[illegible]1..10[illegible]1[illegible]10[illegible]
- -F——[illegible]"{0},{1}" –F "Hello","World"[illegible]

28.4 [illegible]

[illegible]Select-Object[illegible]Format-Table[illegible]Format-List[illegible]

[illegible]

```
@{Label='Column_or_Property_Name';Expression={Value_Expression}}
```

[illegible]“Label”[illegible]“Expression”[illegible]“l”[illegible]“e”[illegible]l[illegible]1[illegible]n[illegible]

```
@{n='Column_or_Property_Name';e={Value_Expression}}
```

[illegible]$_[illegible]

```
@{n='ComputerName';e={$_.Name}}
```

Select-Object[illegible]Format- [illegible]Cmdlet[illegible]n[illegible]name[illegible]label[illegible]l[illegible]e[illegible]Format- Cmdlet[illegible]Width[illegible]Align[illegible]Format-Table[illegible]FormatString[illegible]Format-Table[illegible]

28.5 [illegible]

[illegible]9[illegible]PowerShell[illegible]ByValue[illegible]ByPropertyName[illegible]ByValue[illegible]ByValue[illegible]ByPropertyName[illegible]

[illegible]ByValue[illegible]PowerShell[illegible]gm[illegible]PowerShell[illegible]Cmdlet[illegible]ByValue[illegible]Cmdlet[illegible]Cmdlet[illegible]<String>[illegible]ByValue[illegible]

[illegible]ByValue[illegible]PowerShell[illegible]ByPropertyName[illegible]PowerShell[illegible]

ByPropertyName[illegible]Name[illegible]Status[illegible]ID[illegible]PowerShell[illegible]Cmdlet[illegible]Name[illegible]Status[illegible]ID[illegible]“[illegible]ByPropertyName[illegible]”[illegible]Help[illegible]-Full[illegible]

[illegible]PowerShell[illegible]Get-Service |Stop-Service[illegible]Get-Service | Stop-Process[illegible]Cmdlet[illegible]Cmdlet[illegible]PowerShell[illegible]

[illegible]1[illegible]Cmdlet[illegible]Get-Member[illegible]System.Diagnostics.Process[illegible]Process[illegible]

[illegible]2[illegible]Help <Cmdlet> -Full[illegible]ByValue[illegible]

[illegible]3[illegible]2[illegible]Yes[illegible]2[illegible]——[illegible]4[illegible]2[illegible]“[illegible]”[illegible]4[illegible]

[illegible]4[illegible]Get-Member[illegible]

[illegible]5[illegible]4[illegible]a[illegible]ByPropertyName[illegible]b[illegible]

[illegible]6[illegible]5[illegible]a[illegible]b[illegible]ByPropertyName[illegible]

[illegible]ByValue[illegible]ByPropertyName[illegible]

28.6 [illegible]$_

[illegible]PowerShell[illegible]$_[illegible]

[illegible]PowerShell[illegible]$_[illegible]$_[illegible]——[illegible]$_[illegible]

- [illegible]Where-Object[illegible]

```
Get-Service |3 Where-Object {$_.Status -eq 'Running' }
```

- [illegible]ForEach-Object[illegible]-Process[illegible]

```
Get-WmiObject -class Win32_Service -filter "name='mssqlserver'" |
ForEach-Object -process { $_.ChangeStartMode('Automatic') }
```

- [illegible]Process[illegible]——*Learn PowerShell Toolmaking in a Month of Lunches*[illegible]
- [illegible]28.4[illegible]8[illegible]9[illegible]10[illegible]

[illegible]$_[illegible]$_[illegible]

[illegible]

[illegible]3[illegible] MoreLunches.com [illegible]

[illegible]

[illegible]1[illegible]1—6[illegible]

> **[illegible]** [illegible]PowerShell v3[illegible]PowerShell[illegible]1—6[illegible]

> **[illegible]**
>
> - Sort-Object
> - Select-Object
> - Import-Module
> - Export-CSV
> - Help
> - Get-ChildItem (Dir)

[illegible]1

[illegible]100[illegible]Get-WinEvent[illegible]

[illegible]2

[illegible]VM[illegible]

□□3

□□□□□□□□□□CSV□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□

□□4

□□□□□□□BITS□□□□□□□□□□□□□

□□5

□□□□□□□□□□□□□Win.□□□□C□\□□□□□□□□□□□□□□□□□□□□□
□□□□□Cmdlet□□□□□□

□□6

□□□□C:\Program Files □□□□□□□□□□□□□□□□□□□□□□□□□
C:\Dir.txt□□□□□□□□□□□the >redirector, □□ Out-FileCmdlet□□

□□7

□□□□20□□□□□□□□□□□□□□□□□XML□□□□□□□□□□□□□□□□
XML□□□□□□□□□□□□

> **□□□** □XML□□□□□□□□□□□□□□□□□□□□XML□□□□□□□□□PowerShell □□XML□□□□□□□□□□□XML□□□□□□□Format-Custom□□□□□□XML□□□□□□□□□

□□8

□□□□□□□□□□□□□□□C:\services.csv□□□CSV□□□□

□□9

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□HTML□□□□
HTML□□□□□□□□□□□□□“Installed Services”□

□□10

Get-ChildItem D Shell Shell D

11

12

Shell

13

Shell 11 11

Get-Something 5 11 ID Do-Something

```
Get-Something –id 5 | Do-Something
```

14

15

New-Item Cmdlet C:\Review Mkdir New-Item

16

```
HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User
Shell Folders
```

> **□□□** “User Shell Folders”□□□□□□□□□□□□□□□□□□□□□□“□□”□□□□□□□□□□□□□□□□□□□User Shell Folders □□□□□□□□□□□□□□□□□□□□□Cmdlet□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□17

□□□□□□□□□□□□□□□□□□□□□

- □□□□□
- □□□□□
- □□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□

□□18

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□16□□□□□□□□□□□□

□□□□2□□1—14□

□□□□□□□□□□□□□□□□□□□PowerShell v3□□□□□□PowerShell□□□□□□□□□□□□□□□□□□□□□□□□□□□□□1—14□□□□□

> **□□□**
>
> - Format-Table
> - Invoke-Command
> - Get-Content(or Type)
> - Parenthetical commands
> - @{label='column*header';expression={$*.property}}
> - Get-WmiObject
> - Where-Object
> - -eq -ne -like -notlike

□□1

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ID□□□□□□□□□□□□□□□□□□□□□□

[illegible]2

[illegible]

```
Get-WmiObject -class Win32_UserAccount
```

[illegible]Domain[illegible]UserName[illegible]UserName[illegible]Name[illegible]

```
Domain  UserName
=======  ========
COMPANY  DonJ
```

[illegible]UserName[illegible]Name[illegible]

[illegible]3

[illegible]Localhost[illegible]

```
Get-PSProvider
```

[illegible]

[illegible]4

[illegible]Notepad [illegible]C:\Computers.txt [illegible]

```
Localhost
Localhost
```

[illegible]—[illegible]2[illegible]C:\Computer,txt[illegible]

[illegible]5

[illegible]Win32_LogicalDisk[illegible]DriveType[illegible]3[illegible]

□□□□□□□□□□□□□□□□freespace/size * 100□

□□□Get-WmiObjectcannot □□□□□□□□□□□□□□□□

□□6

□□□root\CIMv2□□□□□□□□□□WMI□□□□

□□7

□□□□□□□□StartMode□Auto□State□□□□Running□
Win32_Service□□□□

□□8

□□□□□□□Email□□□□□□□□□□□□□□□□□□□□

□□9

□□□□□□C:\□□□□□□□□□

□□10

□□□□□□□□□□C:\Users□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□11

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□12

□□□□□□□□Shell□□□□□□10□□

□□13

□□□□□□□□□□□Shell□□□□□□□□

□□14

[illegible]1[illegible]100000[illegible]

[illegible]15

[illegible]

```
Get-WmiObject –Class Win32_Processor
```

[illegible]“MaxSpeed”[illegible]

[illegible]16

[illegible]

```
Get-WmiObject –Class Win32_Process
```

[illegible]Get-Member[illegible]5000[illegible]

[illegible]3[illegible]1—19[illegible]

[illegible] [illegible]PowerShell v3[illegible]PowerShell[illegible]1—19[illegible]

[illegible]

1[illegible]

2[illegible]

3[illegible]${computer name}[illegible]

4[illegible]Shell[illegible]

5[illegible]

6[illegible]

[illegible]

[illegible]1

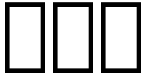
[illegible]ID[illegible]VM[illegible]PM[illegible]C:\Procs.html[illegible]HTML[illegible]HTML[illegible]“Current Processes”[illegible]

[illegible]

[illegible]C:\Services.tdf[illegible]"`t"([illegible]t)[illegible]PoweShell[illegible]

[illegible]3

[illegible]1[illegible]HTML[illegible]Vm[illegible]PM[illegible]MB[illegible]$_.VM / 1MB –as[int]for the VM property[illegible]



[illegible]contact@epubit.com.cn[illegible]

[illegible]ebook@epubit.com.cn[illegible]

[illegible]

- [illegible]@[illegible]
- QQ[illegible]368449889

091507240605ToBeReplacedWithUserId